ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROPUESTA DE DISEÑO DE UN SGSI BASADO EN LA NORMA ISO/IEC 27001. CASO DE ESTUDIO LA EMPRESA ULTRALINK.

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

MARCO VINICIO GUACANÉS CASTRO

marco.guacanes@epn.edu.ec

JONATHAN ALEXANDER VILATUÑA MORALES

jonathan.vilatuna@epn.edu.ec

DIRECTOR: MSc. Pablo Fernando Del Hierro Cadena

pablo.delhierro@epn.edu.ec

CO-DIRECTOR: PhD. Denys Alberto Flores Armas

denys.flores@epn.edu.ec

Quito, Junio 2022

DECLARACIÓN

Nosotros, Marco Vinicio Guacanés Castro con cédula de identidad N.º 1723940175, y Jonathan Alexander Vilatuña Morales, con cédula de identidad N.º 1725263881 declaramos bajo juramento que el presente trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Marco Vinicio Guacanés Castro

C.I:1723940175

Jonathan Alexander Vilatuña Morales

C.I: 1725263881

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Marco Vinicio Guacanés Castro y Jonathan Alexander Vilatuña Morales, bajo nuestra supervisión.

Msc. Pablo Fernando Del Hierro Cadena

DIRECTOR DE PROYECTO

PhD. Denys Alberto Flores Armas

CO-DIRECTOR DE PROYECTO

DEDICATORIA

Dedico este proyecto de titulación a Dios por haberme dado salud y sabiduría las cuales me ayudaron a concluir mi carrera universitaria. A mis padres Nancy Castro y Gonzalo Guacanés quienes siempre fueron un apoyo en mi vida y que, gracias a su esfuerzo, su amor y sacrificio me ayudaron a cumplir esta meta de vida. A mi hermana Cristina la cual estuvo siempre a mi lado y fue una voz de aliento la cual me impulso a salir adelante. A novia Verónica por todo su amor, concejos y ayuda que me brindo durante toda mi carrera. A mis mascotas que siempre estuvieron a mi lado alegrándome y divirtiéndome durante toda la carrera. A mis amigos por siempre estar a mi lado apoyándome de forma incondicional y de forma desinteresada.

Vinicio Guacanés

DEDICATORIA

Dedico este trabajo a mis padres Mélida y Rubén quienes con su apoyo, motivación y esfuerzo me han permitido lograr esta meta, gracias por su ayuda en las adversidades y por creer en mí. A mi hermana Roxana, por darme la valentía y demostrarme que todo es posible si nos enfocamos y esforzamos en una meta, por estar juntos siempre ante toda adversidad y por defendernos el uno al otro ante las injusticias. A mis mascotas en especial a mi gatita y gatitos que siempre estuvieron a mi lado en las noches de desvelo, alegrándome y divirtiéndome con sus locuras, ellos siempre fueron la motivación para levantarme y no rendirme en toda la carrera. A mi mejor amiga Elizabeth, por estar a mi lado dándome fuerzas de manera incondicional y desinteresada.

Jonathan Vilatuña

AGRADECIMIENTOS

En primer lugar, agradecemos a Dios por darnos la vida, salud y sabiduría para poder finalizar nuestro trabajo de titulación y de esta forma poder cumplir una meta más en nuestra vida.

A nuestros padres por estar siempre a nuestro lado y ser nuestro apoyo incondicional durante toda nuestra carrera estudiantil.

A la Escuela Politécnica Nacional y a todos los profesores que tuvimos durante la carrera los cuales con mucha sabiduría y paciencia inculcaron en nosotros los conocimientos, la sabiduría, la honestidad y la responsabilidad para ser un buen profesional.

Al Msc. Pablo Del Hierro y PhD. Denys Flores por guiarnos con sus recomendaciones en la elaboración del presente trabajo.

A la empresa Ultralink por darnos apertura y disponer de sus activos para poder llevar a cabo el presente trabajo.

A nuestros amigos de la universidad por el apoyo brindado durante toda carrera y por no rendirnos frente a las adversidades.

Vinicio Guacanés y Jonathan Vilatuña

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de titulación tiene como objetivo principal la creación del modelo de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC para la toma de decisiones en la empresa Ultralink, basándose en normas y estándares internacionales, acoplándose con la realidad y necesidad de la empresa, para prevenir o reducir los riesgos de seguridad con procedimientos que ayuden al tratamiento de los riesgos, para lograr una gestión adecuada de los activos de información se utilizó las nuevas tecnologías las cuales ayudan a mejorar los procesos de la organización y la atención a que se brinda a los usuarios.

Para la selección de la metodología de tratamiento de los riesgos se realizó una comparativa entre las diferentes metodologías teniendo en cuenta la factibilidad de su implementación en la empresa y los beneficios que está metodología aportaría a la misma por lo antes mencionado se seleccionó a Magerit.

El presente documento tiene 5 capítulos y en cada uno se describen temas de apoyo para desarrollar el presente trabajo. Al finalizar el proyecto, se pudo identificar los activos críticos de la organización, las amenazas y vulnerabilidades a las cuales están expuestos los activos, también se logró definir las políticas que se pueden implementar en la empresa teniendo en cuenta los dominios, controles y objetivos del Anexo A de la norma ISO 27001. También se generó un plan de tratamiento de riesgos donde se pueden evidenciar las acciones recomendadas que la organización puede tomar para minimizar los riesgos.

Palabras clave: Sistema de Gestión de Seguridad de la Información, ISO27001: 2013, Gestión de Riesgos, Magerit, Metodologías para la gestión de riesgos.

ABSTRACT

The main objective of this degree work is the creation of a model of an information security management system (ISMS) based on the ISO/IEC standard for decision making in the Ultralink company, based on international norms and standards, coupled with the reality and need of the company, to prevent or reduce security risks with procedures that help the treatment of risks, to achieve proper management of information assets new technologies were used which help to improve the processes of the organization and the attention provided to users.

For the selection of the risk treatment methodology, a comparison between the different methodologies was made, taking into account the feasibility of its implementation in the company and the benefits that this methodology would bring to the company, for which Magerit was selected.

This document has 5 chapters and each one describes support topics to develop this work. At the end of the project, it was possible to identify the critical assets of the organization, the threats and vulnerabilities to which the assets are exposed, it was also possible to define the policies that can be implemented in the company taking into account the domains, controls and objectives of Annex A of ISO 27001. A risk treatment plan was also generated where the recommended actions that the organization can take to minimize risks can be evidenced.

Keywords: Information Security Management System, ISO27001: 2013, Risk Management, Magerit, Methodologies for risk management.

CAPITULO I INTRODUCCIÓN

1.1. Introducción

Hoy en día la información es uno de los activos más importantes y esenciales para cualquier organización ya que está adquiere valor cuando es utilizada de forma adecuada, responsable y segura. El aseguramiento y la protección de la información que poseen las organizaciones representan un reto al momento de garantizar su integridad, disponibilidad y confidencialidad razón por la cual la seguridad de la información ha llegado a ser uno de los aspectos de mayor preocupación a nivel mundial.

Toda organización debe ser consciente de las vulnerabilidades y amenazas que existen actualmente, ya que estas atentan contra la seguridad y privacidad de la información y al materializarse pueden acarrear problemas a la empresa como la afectación en la reputación de la imagen, costos económicos, sanciones legales, etc. Por lo tanto, las organizaciones deben velar por la seguridad y protección de la infraestructura, recursos e información implementando y mejorando constantemente medidas de seguridad las cuales estén orientadas a detectar y prevenir los riesgos que pueden llegar a comprometer los activos de información.

Hoy en día debido a los múltiples riesgos y amenazas que atentan contra la seguridad, la protección y privacidad de los datos, es primordial que las organizaciones establezcan, implementen y mantengan un Sistema de Gestión de Seguridad de la Información, el cual este alineado con los objetivos estratégicos y necesidades del negocio y de sus partes interesadas. Por lo tanto, el presente trabajo busca diseñar un Sistema de Gestión de Seguridad de la Información, el cual proporcionará un marco metodológico que está basado en buenas prácticas, las cuales son un mecanismo eficaz para gestionar las amenazas y vulnerabilidades a las cuales pueden estar expuestos los activos de información que posee una organización. En la actualidad la empresa Ultralink no posee políticas, normas y controles sobre cómo proteger sus activos de información y que acciones realizar cuando se materialice una amenaza en la organización, por lo cual se debería

implementar un Sistema de Gestión de Seguridad de la Información de forma inmediata.

1.2. Planteamiento del Problema

El avance tecnológico ha permitido a las empresas implementar, herramientas y estrategias que permiten proteger la información y los sistemas informáticos ya que las grandes, medianas o pequeñas empresas son blancos de ataques informáticos como: denegación de servicios, suplantación de identidad, SPAM, encriptación de la información, daños de los equipos informáticos, etc. Al analizar la infraestructura del departamento de TI de una PYME, es notable el crecimiento en dicha área al pasar de los años, por lo cual es necesario implementar controles a nivel de seguridad de la información para garantizar la disponibilidad, integridad, y confidencialidad de la información, para así proteger los recursos tecnológicos, base de datos, servidores, información sensible, aplicativos y equipos de la organización. Sin embargo, las Pymes en el Ecuador no cuentan con un SGSI implementado el cual pueda velar por la seguridad de la información [1].

Una causa importante de la ausencia de un SGSI en las Pymes en Ecuador es el aspecto económico, porque el costo de realizar la implementación del SGSI es alto, lo cual no permite que las pequeñas empresas puedan ejecutarlo. Otro motivo de la falta de un SGSI en las Pymes es la falta de información sobre los beneficios y ventajas que éste proporciona a las empresas, lo que genera una falta de interés en la implementación de un SGSI.

Por su parte en la empresa Ultralink, aunque posee recursos tecnológicos, presenta problemas entre los que se destaca la inexistencia de procesos sobre gestión de la información, gestión de los recursos físicos, gestión de políticas de seguridad, manejo de inventarios, control de equipos, no posee un mapa de análisis de riesgos y controles de los mismos, no cuenta con un sistema de gestión de incidentes de seguridad de la información, por lo antes mencionado se puede decir que Ultralink no cuenta con un Sistema de

Gestión de Seguridad de la información, lo que impide a la empresa prestar un servicio con las especificaciones y estándares internacionales.

1.3. Justificación

Hoy en día, la información es el activo más importante que proteger en toda empresa, debido a esto se debe implementar procedimientos o controles de seguridad los cuales ayuden a las organizaciones a minimizar los riesgos en su trabajo diario.

El diseño de un Sistema de Gestión de Seguridad de la Información que está basado en un modelo de buenas prácticas de seguridad, como es la norma ISO/IEC 27001:2013, proveerá a la empresa las condiciones necesarias para que la seguridad de la información cumpla los objetivos estratégicos que posee la empresa. Un Sistema de Gestión de Seguridad de la Información, demuestra el compromiso que tiene la organización con la seguridad de la información y provee los elementos necesarios para gestionar los riesgos que puedan atentar contra la seguridad de la información, lo cual genera confianza en las partes interesadas.

También la incorporación de un Sistema de Gestión de Seguridad de la Información le permitirá a la empresa fortalecer los pilares de la seguridad con lo cual se da cumplimiento a los principios de la integridad, confidencialidad y disponibilidad de la información lo cual ayuda a fomentar y extender en toda la organización una cultura apropiada de seguridad de la información.

El presente proyecto busca conocer el estado actual de la organización, para así evidenciar las brechas de seguridad que la empresa posee y de esta forma poder dar solución a las vulnerabilidades y disminuir el riesgo de que se materialicen y puedan afectar a los servicios que ofrece la empresa Ultralink. También, se busca generar una base de conocimientos los cuales puedan ser de ayuda ante una amenaza que ya se ha materializado con anterioridad y se la pueda mitigar en el menor tiempo posible.

1.4. Objetivos

1.4.1. Objetivo general

- Diseñar un modelo de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001: 2013 para ayudar a la toma de decisiones en la empresa Ultralink.

1.4.2. Objetivos específicos

- Recopilar y evaluar toda la información existente y establecer procesos sobre la Gestión de Seguridad de la información en la empresa Ultralink.
- Generar un informe técnico que permita identificar, analizar y evaluar los riesgos y amenazas a los que se expone las TICs en la organización.
- Proponer acciones correctivas mediante una metodología para reducir el riesgo de amenazas que puedan afectar a la información y equipos de la empresa en base a estándares y buenas prácticas.

1.5. Alcance

El presente trabajo tiene como objetivo diseñar un Sistema de Gestión de la Seguridad de la Información bajo el estándar ISO 27001:2013 para la empresa Ultralink, la cual brinda servicios de telecomunicaciones y conectividad a través de redes e infraestructura actualizada y moderna, cumpliendo con las normativas vigentes y de esta forma logrando que todos los habitantes de la provincia de Pichincha puedan acceder al servicio de datos e internet bajo la premisa de calidad y precio asequible.

Para el desarrollo del proyecto se utilizará como guía principal la norma ISO-IEC:27001: 2013 que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implementar, mejorar y mantener un SGSI [2].

El alcance del proyecto abarcará el análisis y diseño del Sistema de Gestión de Seguridad de la Información para la empresa Ultralink, basado en la norma

ISO/IEC:27001: 2013, pero no cubre las fases de implementación, revisión, mejora y mantenimiento del Sistema de Gestión de Seguridad de la Información, igualmente en el alcance se abarcara la elaboración de unas plantillas sobre las políticas que puede implementar la empresa y una guía donde se describirán algunas consideraciones a tener en cuenta antes de la implementación del modelo de SGSI. También se pretende demostrar que el modelo elaborado es aplicable en una organización y sobre todo que sirva como ejemplo para futuras implementaciones.

CAPITULO II MARCO REFERENCIAL Y METODOLÓGICO

2.1. Marco teórico

2.1.1. Seguridad de la información

La seguridad de la información es un conjunto de medidas y métodos que se utilizan para proteger y controlar los datos que se procesan dentro de una organización y de esta forma asegurar que los datos no salgan del sistema que ha sido establecido por la organización. Es muy importante el entender que cualquier organización, independientemente de su tamaño posee datos confidenciales de sus clientes, empleados o socios y por este motivo se debe establecer medidas de seguridad necesarias para garantizar la protección y el correcto tratamiento de los datos [3].

Para lograr el aseguramiento de la información se debe implementar controles los cuales nos ayuden a analizar, organizar, monitorear y mejorar el procesamiento de la información. La norma ISO 27001: 2013 establece un modelo para implementar un sistema de gestión de seguridad de la información. El objetivo principal que persigue esta norma es proteger los activos de información, es decir los equipos, usuarios e información. Para establecer este sistema de seguridad de la información ISO, se deben considerar tres pilares básicos de seguridad los cuales son conocidos como CIA (Confidentiality-Integrity-Availability) o “La Triada de la seguridad”. A continuación, en la Figura 1 se muestran los tres pilares sobre los cuales se aplican las medidas de protección de la información.

Figura 1. Pilares de la Seguridad de la Información.

Fuente: Autores del Proyecto

- **Integridad:** Hace referencia a la validez y precisión con que la información es almacenada, controlando las modificaciones que se realizan sobre esta.
- **Disponibilidad:** Es la propiedad que posee la información para ser utilizada en el momento en que esta sea requerida.
- **Confidencialidad:** Es la característica de asegurar que determinada información llegue únicamente al personal o persona autorizada.

2.1.1.1. Gestión de riesgos de seguridad de la información

Para facilitar el proceso de análisis y evaluación de riesgos, es importante comprender los siguientes conceptos básicos:

- **Amenaza:** Es la posible causa de un accidente inesperado el cual puede generar daños a los sistemas, persona u organización. Estas amenazas pueden ser naturales o causadas [3].
- **Vulnerabilidad:** Es la debilidad que posee un activo o control, esta puede ser explotada por una o más amenazas y de esta forma causar daños.
- **Riesgo:** Es la probabilidad de que una amenaza pueda aprovechar una vulnerabilidad y de esta manera causar la pérdida o daño de un activo o información. Existen dos tipos de riesgos los cuales son [3]:
    - **Riesgo inherente:** Es el riesgo que existe en cada actividad sin la ejecución de ningún control.
    - **Riesgo residual:** Es el riesgo que permanece tras la implementación del tratamiento del riesgo.
- **Impacto:** Es el resultado de la materialización de la amenaza.

2.1.1.1.1. Proceso de gestión de riesgos de seguridad de la información

El proceso de gestión de riesgos de seguridad de la información puede poseer actividades iterativas de evaluación y/o tratamiento de riesgos, el enfoque iterativo de la evaluación de riesgos potenciales puede mejorar el detalle de la valoración con cada iteración. Un enfoque iterativo proporciona un buen equilibrio entre la reducción del tiempo y los esfuerzos que se necesitan para identificar los riesgos de alto impacto [4].

Las actividades que se deben realizar para la gestión de los riesgos son:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Los pasos y actividades que se debe desarrollar para tener una correcta gestión de los riesgos son las siguientes [4]:

Tabla 1. Proceso para la gestión de los riesgos

Actividades	Pasos
Establecimiento del contexto	1. Levantamiento la información inicial 2. Creación de los criterios para la gestión de los riesgos 3. Definición de los límites y el alcance que se tendrá en la gestión de riesgo 4. Creación de una organización para las operaciones del SGSI
Valoración del riesgo	5. Identificación de los activos de información 6. Identificación de las amenazas y vulnerabilidades 7. Identificación de los controles existentes 8. Identificación y valoración de las consecuencias

	9. Valoración de los incidentes 10. Determinación del nivel de estimación del riesgo 11. Evaluación del riesgo
Tratamiento del riesgo	12. Selección de controles
Aceptación del riesgo	13. Aceptación del riesgo
Comunicación del riesgo	14. Comunicación del riesgo
Monitoreo y revisión del riesgo	15. Monitoreo y revisión de los riesgos

Fuente: [4]

A continuación, en la Figura 2 se muestra el proceso iterativo que se debe tener en cuenta para la gestión de los riesgos.

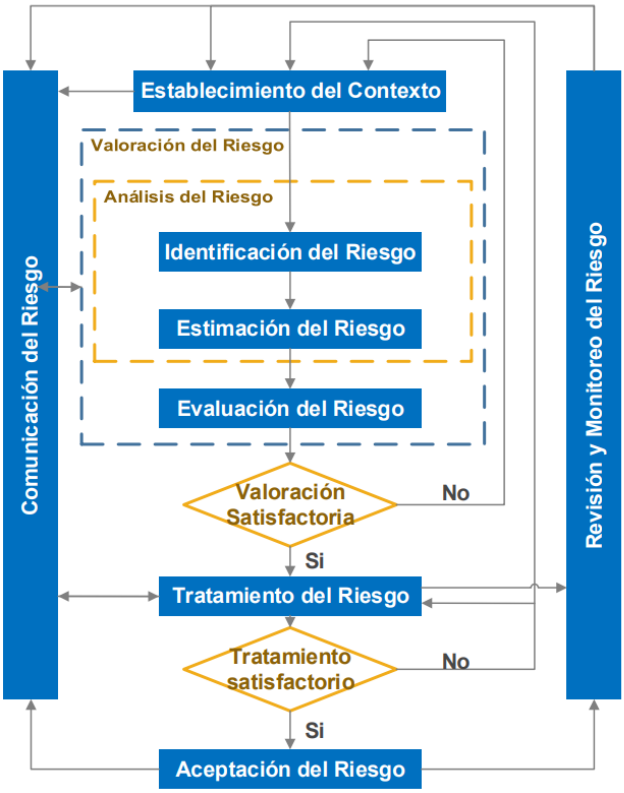


Figura 2. Proceso de gestión del riesgo en la seguridad de la información.

Fuente: ISO 27005

2.1.1.1.2. Beneficios de la Gestión de riesgos

Entre los beneficios que se obtiene al gestionar los riesgos tenemos:

- Reducir los números de incidentes e impactos que estos pueden causar a la organización.
- Se alinean los requerimientos de seguridad con los del negocio.

- Se genera una mejora continua en el proceso de análisis y tratamiento de los riesgos.
- Se produce una conciencia de seguridad y da tranquilidad a las partes interesadas.
- Se obtiene una visión completa de los riesgos con lo cual se puede generar una planeación estratégica para la toma de decisiones.

2.1.1.2. Gestión de Incidentes de la seguridad de la información

Hoy en día, los incidentes de seguridad de la información parecen inevitables, por lo que nos toca plantearnos como gestionaremos dichos incidentes de forma eficaz y ágil para la organización.

La norma ISO 27001:2013 permite establecer controles para gestionar los incidentes de seguridad de la información, estos controles permiten garantizar un enfoque eficaz y constante lo cual facilita la comunicación entre los eventos de seguridad y las debilidades.

Un análisis de riesgos no puede concluir con la eliminación total de las vulnerabilidades, pues esto no sería práctico o viable por lo que las vulnerabilidades residuales siempre existen, por lo que se tendrá incidentes en la seguridad de la información, además de que puedan surgir amenazas o vulnerabilidades no identificadas hasta ahora [5].

Por lo antes mencionado se debe implementar una herramienta para la gestión de los incidentes de la seguridad de la información tomando en cuenta los siguientes objetivos generales:

- Detectar, evaluar e informar los incidentes.
- Responder ante incidentes.
- Reportar las vulnerabilidades.
- Aprender de los incidentes de la seguridad.

2.1.1.2.1. Pasos para la resolución de incidentes

Para realizar una correcta gestión de los incidentes se debe tener en cuenta a los siguientes pasos que se muestran en la Figura 3:

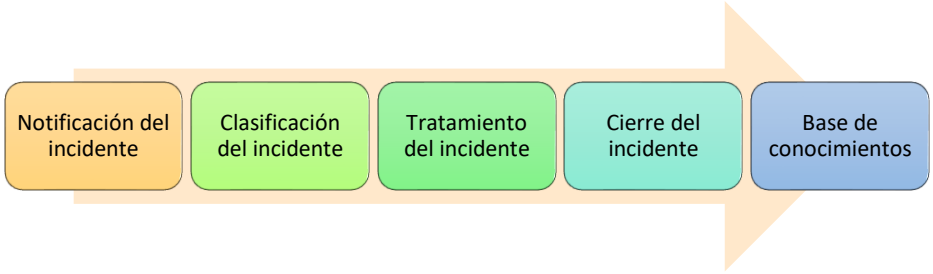


Figura 3. Pasos para la resolución de incidentes

Fuente: Autores del proyecto

1. **Notificación del incidente:** En este paso se informa a la organización sobre el incidente**,** generalmente esto se lo realiza mediante llamada telefónica, correos, herramientas de software, etc. [5]
2. **Clasificación del incidente:** El personal que recibe la notificación clasifica al incidente basándose en diversos parámetros.
3. **Tratamiento del incidente:** Una vez se conoce la gravedad del incidente se establece un tiempo acorde para la solución.
4. **Cierre del incidente:** Una vez se soluciona el incidente se procede a realizar un registro en el cual se incluya toda la información que se generó en el tratamiento del incidente, también se notifica a la persona que realizo la notificación.
5. **Base de conocimientos:** Es la base que almacena todos los registros de los incidentes que se han generado, esta base es muy importante ya que si un incidente que ya ha sido mitigado se genera a futuro se posee la solución de este sin perder tiempo [5].

2.1.2. Normas ISO/IEC 27000

Las normas de la serie ISO / IEC-27000 son un conjunto de estándares que fueron creados y administrados por la ISO (Organización

Internacional de Normalización) y el IEC (Comité Internacional de Electrónica). La serie 27000 tiene como objetivo establecer buenas prácticas las cuales están relacionadas con la implementación, mantenimiento y gestión del SGSI (Sistema de Gestión de Seguridad de la Información). Estos lineamientos tienen como objetivo establecer las mejores prácticas en diferentes aspectos relacionados con la gestión de la seguridad de la información, y están orientados a la mejora continua y la reducción de riesgos.

2.1.2.1. Estándares que componen la ISO 27000

La ISO (Organización Internacional de Estandarización) recoge un extenso número de normas dentro de la familia de ISO 27000, Esta estandarización incluye definiciones y términos que se utilizarán a lo largo de la serie 27000 los cuales tienen como objetivo establecer buenas prácticas para la implementación, mantenimiento, gestión y mejora de un SGSI (Sistema de Gestión de Seguridad de la Información). A continuación, en la Tabla 1 se detallarán las mismas [6]:

Tabla 2. Normas ISO 27000.

Norma	Alcance	Fecha de Publicación	Características
27001	Requisitos para un SGSI	15 de octubre de 2005	Este estándar cubre todos los requisitos de los SGSI en las organizaciones. La ISO 27001 reemplaza a BS 7799-2 y especifica los requisitos de adaptación para empresas certificadas.
27002	Guía de buenas prácticas	1 de julio de 2007	En esta guía se describe los objetivos de control y las evaluaciones de seguridad de la información recomendadas. Hay 39 objetivos de control y 133 controles agrupados en 11 áreas diferentes.
27003	Manual de implementación de un SGSI	1 de febrero de 2010	Es un manual para implementar un SGSI, nos provee la información necesaria para la utilización del ciclo PHVA (Planificar, Hacer, Verificar y Actuar). El origen de esta norma se encuentra en el Anexo B de la norma BS7799-2.

27004	Guía para la utilización de métricas y técnicas para determinar la eficacia de un SGSI	15 de diciembre de 2009	Las métricas se utilizan para la medición de los componentes de las fases “implementar y utilizar” que posee el ciclo Deming.
27005	Normativa para la gestión de los Riesgos en la Seguridad de la Información	15 de junio de 2008	Es un estándar que está diseñado para ayudar a implementar un enfoque basado en la seguridad de la información para la gestión de riesgos. Esta Norma puede aplicarse a todo tipo de organizaciones que pretendan gestionar todos los riesgos potenciales.
27006	Estándar que especifica los requisitos para la acreditación de las entidades de auditoría y certificación de SGSI	1 de marzo de 2007	Esta es una versión revisada de EA-7/03 (Requisitos para la acreditación de organismos), esta norma permite que todas las normas de acreditación ISO / IEC 17021 aplicadas en los organismos de certificación se interpreten según la norma ISO 27001.
27007	Manual de auditoría de un SGSI	14 de noviembre de 2011	Es un manual de auditoría de un SGSI. Este estándar ha sido creado para proveer un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.
27011	Guía de gestión de seguridad de la información para telecomunicaciones	15 de diciembre de 2008	Está guía está orientada a los organismos que generan procesos de apoyo e información en las instalaciones de redes y líneas de telecomunicaciones.
27017	Guía de seguridad para Cloud Computing	15 de diciembre de 2015	Está guía esta alineada con la ISO 27002 y con los controles de los entornos en la nube.
27018	Código de buenas prácticas para los proveedores de servicios de cloud computing	29 de Julio de 2014	Es un código de protección de datos para los proveedores de servicios de cloud computing.
27031	Guía de continuidad del negocio referente a las TI	1 de marzo de 2011	Explica los principios y conceptos de las tecnologías de la información y la comunicación (TIC), los prepara para las tareas comerciales y describe los procesos y métodos necesarios para indicar e identificar todos los aspectos de la mejora de la preparación de las TIC de la empresa para garantizar la continuidad del negocio.
27032	Guía para la mejora del estado de seguridad cibernética	16 de julio de 2012	Esta guía establece una descripción general de Seguridad Cibernética, también proporciona un marco seguro

			para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos.
27033	Guía de seguridad de la red	15 de diciembre de 2009	En esta guía se proporciona una visión amplia sobre la seguridad de la red y los conceptos asociados a las mismas.
27034	Guía de seguridad en aplicaciones.	21 de noviembre de 2011	Norma dedicada a la seguridad en las aplicaciones informáticas en la cual se toma en cuenta los conceptos generales del proceso de gestión de seguridad y validación de la seguridad en las aplicaciones.
27035	Guía sobre la gestión de incidentes de seguridad en la información	17 de agosto de 2011	Proporciona una guía la cual está constituida por los principios en la gestión de incidentes, guías para la elaboración de planes de respuesta ante incidentes y guía de respuesta ante incidentes.

Fuente: Autores del Proyecto

2.1.2.2. Beneficios de la norma ISO/IEC 27000

Los beneficios que obtiene una organización al implementar este tipo de normas son muy amplios, a continuación, se menciona algunos de los mismos:

- Mejora la imagen de la organización ya que indica a los proveedores, clientes y grupos de interés que la seguridad es una de las prioridades de la empresa [7].
- Se realiza el cumplimiento de las normativas legales relativas a la protección de datos.
- Permite generar una evaluación integral de los riesgos que pueden afectar a la empresa [7].
- Reduce la pérdida o robo de información.
- Ayuda a la identificación de las áreas del sistema que poseen debilidades.
- Permite crear y manejar un registro de las amenazar y vulnerabilidades.

- Reduce la probabilidad y el impacto que pueden ocasionar incidentes.

2.1.3. Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es una herramienta la cual tiene como objetivo velar por la seguridad de la información. En esta herramienta se incluyen todas las políticas, procedimientos, directrices, así como los recursos y actividades relacionadas que son administradas por la organización.

Desde el punto de vista de la norma internacional ISO/IEC 27001: 2013 el SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y de esta forma lograr sus objetivos comerciales [8].

El alcance que puede tener un SGSI, depende de la ubicación de los activos de información importantes, la aplicación de esta herramienta puede incluir solo una parte de la organización y funciones específicas o a toda la organización y sus funciones.

Cada organización puede aplicar un SGSI según sus necesidades ya que a las tres características básicas iniciales de la seguridad se pueden incluir otras adicionales como la trazabilidad, autenticidad, auditabilidad, no repudio, etc. según se considere adecuado para cumplir con los requerimientos internos y externos de la organización [8].

2.1.3.1. Beneficios de un SGSI

Los beneficios que obtiene las empresas al implementar un SGSI son [8]:

- Reduce el riesgo de pérdida de información en las organizaciones.
- Se realizan evaluaciones de forma periódica lo cual deja en evidencia los riesgos a los cuales están expuestos los clientes.
- Es un método que permite administrar la seguridad de la información de forma clara y precisa.

- Focaliza el gasto de los recursos en donde producen una mayor ventaja.
- Implementa medidas de seguridad para que solo los clientes pueden acceder a la información.
- Permite a las organizaciones continuar operando normalmente en caso de generarse un problema.
- Puede realizar una integración general con otros sistemas de gestión estándar como: ISO 9001, ISO 14001, OHSAS 18001, entre otros [8].
- La organización cumple con la ley vigente para la información personal y la propiedad intelectual.
- Promueve la reducción de costos y una mejor operación de los procesos.
- Al contar con un SGSI se mejora la imagen de la empresa tanto nacional como internacional.
- El SGSI se encarga de proteger todo conjunto de datos que genera valor a la empresa, ayudando a que los riesgos sean conocidos, asumidos, gestionados y minimizados de forma documentada y adaptable [8].

2.1.3.2. Implantación de un SGSI

La implementación de un SGSI es una decisión en la cual se debe involucrar a toda la organización, y debe ser apoyado y guiado por la alta dirección de la empresa. Además, el diseño dependerá de la infraestructura, las necesidades y los objetivos de la empresa, los elementos antes mencionados son los que ayudaran a definir de forma correcta el alcance de la implementación del SGSI [9].

Para facilitar el proceso de implementación, lo mejor es contar con la ayuda de la empresa, la cual ayudara en el asesoramiento durante todo el proceso, especialmente en el primer año.

El tiempo que se necesita para realizar la implementación de un SGSI varía dependiendo del tamaño de la empresa, de los recursos asignados y del estado inicial de la seguridad de la información.

El método que se utiliza para medir y evaluar los resultados debe estar en una evolución continua, ya que será la base de cualquier sistema de gestión de la seguridad información. Por lo tanto, para su implementación es necesario utilizar el modelo PDCA [9].

2.1.3.3. Ciclo de Deming o ciclo PDCA

El nombre de ciclo PDCA se deriva de las siglas en inglés Plan, Do, Check, Act, también se le llama ciclo de Deming porque su autor es Edwards Deming o ciclo de mejora continua. Esta metodología describe los cuatro pasos básicos que se deben implementar de manera sistemática para lograr la mejora continua es decir la reducción de fallas, mejora de la eficiencia y efectividad, resolución de problemas y eliminación de riesgos potenciales.

Como se mencionó anteriormente el Ciclo Deming consta de 4 etapas por lo que una vez completada la etapa final y analizado los resultados obtenidos se debe volver a la primera etapa y repetir el ciclo nuevamente para poder reevaluar periódicamente las actividades para incorporar nuevas mejoras [10].

Las fases que se indican en la Figura 4 se las detallará a continuación:

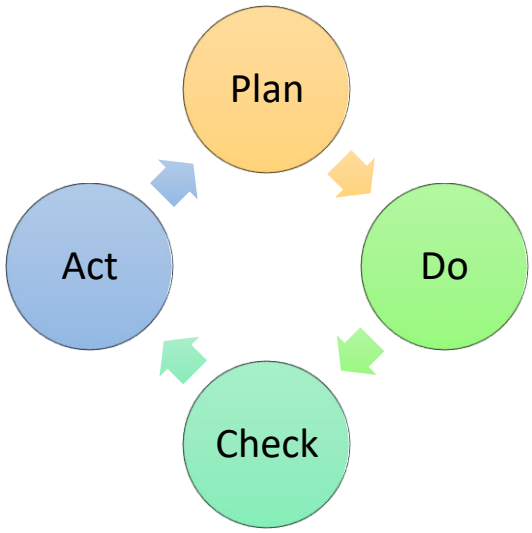


Figura 4. Ciclo PDCA

Fuente: [10]

- **Plan (Planear):** Es la fase inicial en la cual se establece el SGSI, es decir se crean las estrategias, políticas, objetivos, procesos y procedimientos relativos a la gestión de los riesgos y la mejora de la seguridad de la información que posee la organización.

- **Do (Hacer):** En esta fase se implementa y gestiona el SGSI teniendo en cuenta los controles, procedimientos y procesos seleccionados en la fase inicial, si es posible esta implementación debe ser realizada en un entorno de pruebas con lo cual se verificas los resultados antes de generar la implementación en el sistema real. También en esta fase se debe establecer cuál va a ser el encargado de ejecutar las tareas que se le delego [11].

- **Check (Verificar):** Esta tercera fase se encarga del monitoreo y revisión del SGSI, es decir en esta fase se comprueba si las medidas que se han adoptado han surtido efecto por lo cual se debe recopilar datos y monitorizar el comportamiento del sistema.

- **Act (Actuar):** La fase final se encarga del mantenimiento y mejora del SGSI por lo cual se deben adoptar acciones preventivas y correctivas teniendo con objetivo mejorar el SGSI. En caso de haber ocurrido algún mal funcionamiento, se deberá repetir el ciclo de nuevo.

Con respecto a la ISO 27001: 2013 se establece que la Gestión de la Mejora Continua es obligatoria, pero no es obligatorio utilizar el modelo PDCA lo cual genera una mayor flexibilidad para usar cualquier otro modelo. Teniendo en cuenta que el ciclo PDCA y el enfoque de uso están incluidos en la ISO 27001: 2013 se propone un nuevo enfoque basado en los procesos, lo cual alinea la mejora continua con los objetivos de alcanzar el más alto nivel de desempeño en la empresa. A continuación, en la Figura 5 se muestra una representación gráfica del ciclo PDCA y la relación que este tiene con la estructura general de ISO 27001: 2013 [11].

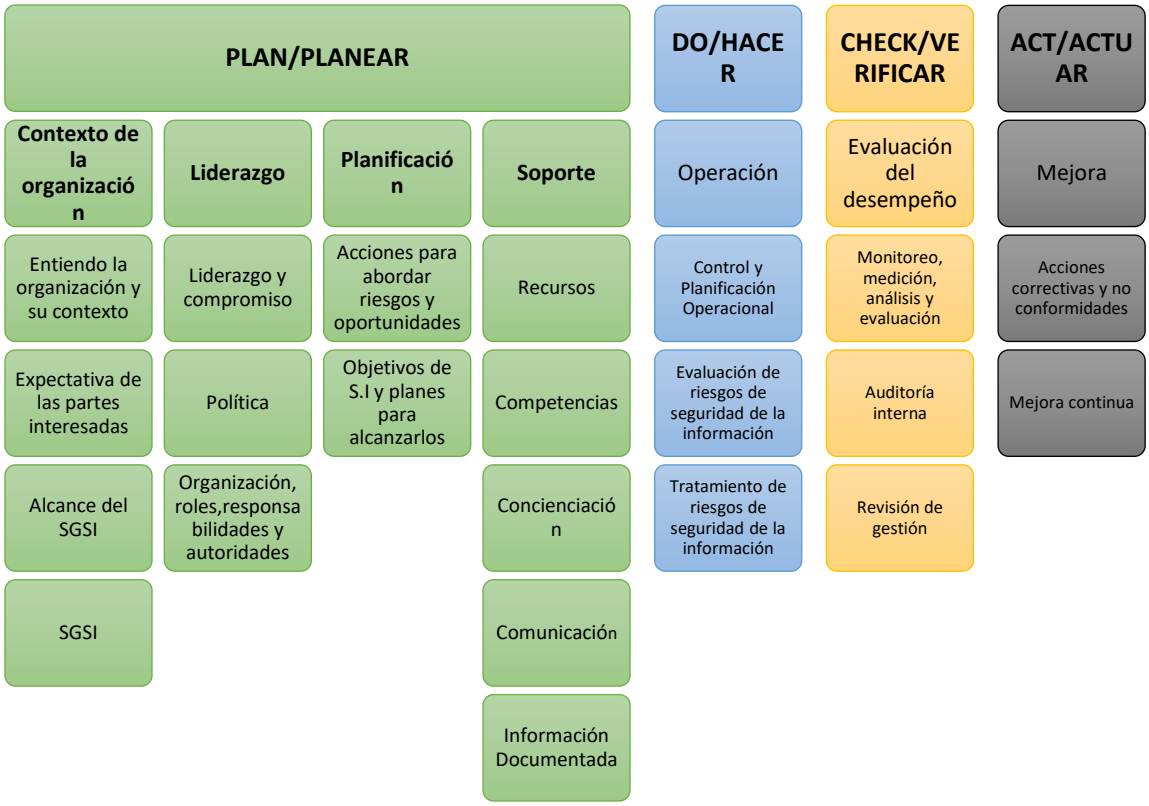


Figura 5. ISO 27001: 2013 Y CICLO PDCA

Fuente: Autores del proyecto

2.2. Metodologías

2.2.1. Metodologías para la Gestión de Riesgos

Los métodos de análisis de riesgos son técnicas las cuales se emplean para evaluar los riesgos de un proceso o proyecto. Estos métodos ayudan a tomar decisiones las cuales permiten implementar medidas de prevención contra peligros potenciales o reducir su impacto. No existe una única metodología de gestión por lo cual la forma ideal de realizar este control es mediante la combinación de las metodologías según las necesidades del negocio o proyecto [12].

Las metodologías están constituidas por principios de gestión de riesgos los cuales son parte fundamental para la organización ya que estos ayudan a identificar los puntos débiles de las estructuras informáticas, son una guía que permiten elegir medidas de protección y también permiten adaptar las políticas de seguridad a las necesidades de las organizaciones.

En el campo de la seguridad informática, las metodologías de análisis de riesgos se constituyen a partir del SGSI que posee la organización, estas metodologías utilizan una serie de modelos y procesos para realizar escaneos de vulnerabilidades, posterior a los escaneos se puede gestionar la información y los recursos de TI de forma adecuada. Existen diversos métodos de análisis de riesgos, entre los que destacan los siguientes [12]:

2.2.1.1. MAGERIT

MAGERIT es una metodología que fue desarrollado por el Consejo Superior de Administración Electrónica de España, este método de análisis y gestión de riesgos ayuda a minimizar los riesgos que trae la implementación y el uso de las Tecnologías de la Información. Los principales elementos para el análisis de riesgos que toma en cuenta MAGERIT son: los activos, las amenazas, las vulnerabilidades, el impacto, los riesgos y las salvaguardias [12].

Los objetivos que persigue esta metodología son:

- Concientizar a los responsables de las organizaciones sobre la existencia de riesgos y de la necesidad de gestionarlos
- Proporcionar un análisis sistemático de los riesgos derivados del uso de las tecnologías de la información y la comunicación.
- Ayudar en la detección oportuna y planificación del tratamiento para mantener los riesgos controlados.
- Preparar a la Organización para procesos de auditorías, evaluación, certificación o acreditación, según corresponda [13].

Esta metodología está estructurada por tres libros los cuales son:

- **Libro 1- Método:** Esta conformado por ocho capítulos los cuales van desde una introducción de la metodología hasta consejos prácticos los cuales se los puede aplicar en el análisis de los riesgos.

- **Libro 2 - Catálogo de Elementos:** Es un complemento al capítulo anterior, en este se busca estandarizar los tipos de activos, los criterios y dimensiones de valoración, las amenazas y las salvaguardas. También trata de homogenizar los resultados [13].
- **Libro 3 – Guía Técnicas:** Describe algunas técnicas utilizadas en el análisis y la gestión de los riesgos.

2.2.1.2. OCTAVE

La metodología OCTAVE se deriva de las siglas Operational Critical, Threat, Asset and Vulnerability Evaluation, fue desarrollado para el Departamento de Defensa de los Estados Unidos en la Universidad Carnegie Mellon (CMU). Existen dos versiones: OCTAVE-S, una metodología simplificada para organizaciones pequeñas y OCTAVE Allegro la cual es una versión más completa para organizaciones grandes las cuales poseen estructuras multinivel [14].

A diferencia de otros métodos de evaluación OCTAVE se basa en el riesgo operativo y las prácticas de seguridad. Está metodología está diseñada para permitir a las organizaciones:

- Administrar y gestionar la evaluación de riesgos de seguridad de la información.
- Tomar mejores decisiones basados en sus riesgos únicos.
- Centrarse en la protección de activos clave.
- Comunicar de manera eficaz la información de seguridad.

OCTAVE se organiza en base a tres aspectos básicos los cuales permiten a la organización tener una imagen completa de las necesidades de seguridad de la información. En la Figura 6 se detalla de mejor manera cuales son estos tres aspectos.

Figura 6. Fases de OCTAVE

Fuente: Autores del Proyecto

En la fase 1 se realiza la identificación de los activos más importantes que posee la empresa, posterior a la identificación se evaluaran para realizar una clasificación de estos y gracias a esta evaluación se puede determinar las amenazas y vulnerabilidades a las cuales están expuestos estos activos [15].

En la fase 2 se realiza un análisis de la infraestructura que posee la empresa para poder determinar las amenazas que pueden ser una amenaza para la seguridad.

En la fase final se encuentra el personal que se encargara del análisis de los riesgos los cuales se encargaran de realizar la evaluación a todas las amenazas y riesgos, también se encargaran de desarrollar un plan de mitigación en el cual se implementes los controles que permitan disminuir los niveles de riesgos [15].

2.2.1.3. NIST SP 800:30

Es una guía la cual fue propuesta por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos del sistema de tecnología de la información. Esta guía es un conjunto de recomendaciones y pautas para una adecuada gestión de riesgos, para el uso de esta guía es recomendable el apoyo de toda la organización para de esta forma cumplir de forma eficiente los objetivos de la gestión de riesgos. La metodología NIST SP 800:30 consta de los siguientes pasos de análisis de riesgo [12]:

- Caracterización del sistema
- Identificación de amenazas
- Identificación de vulnerabilidades
- Control analítico
- Identificación de riesgos
- Análisis de impacto
- Identificación y evaluación de riesgos
- Recomendaciones de control

NIST se distingue por gestionar los riesgos en proyectos de TI donde logra niveles satisfactorios en software, hardware, BD, redes y telecomunicaciones. Sin embargo, al ser una metodología tan potente, esta característica se convierte en una limitación al momento de su aplicación en pequeñas empresas con altas limitaciones de personal [12].

2.2.1.4. CRAMM

Proviene de las siglas CCTA Risk Analysis and Management Method, es una metodología de análisis de riesgos que fue desarrollada en Reino unido por el Central Communication and Telecommunication Agency (CCTA). Esta metodología está dirigida hacia las grandes industrias como las organizaciones gubernamentales, el mantenimiento y gestión de esta metodología está a cargo de la empresa privada de consultoría Insight Consulting [16]. CRAMM se compone de tres etapas para el análisis de riesgos las cuales son:

Fase 1: Establecimiento de los objetivos de seguridad

- Se define el alcance.
- Se define el valor de la información en función del impacto que causaría si esta es corrompida, para la obtención de estos valores se realiza entrevistas a los usuarios.

- Se identifican y valoraron los activos físicos que conformen el sistema.
- Se identifican y valoraron los activos de software que conformen el sistema.

Fase 2: Evaluación de riesgos [16]

- Se identifica y valora el nivel de las amenazas que pueden afectar al sistema.
- Se valora las vulnerabilidades de los sistemas ante las amenazas que han sido identificadas.
- Se calcula el riesgo en base a las valoraciones de las amenazas y vulnerabilidades.

Fase 3: Identificación y selección de contramedidas

- Se documenta el inicio del proyecto.
- Se crean informes sobre el análisis de riesgos.
- Se crean informes sobre la gestión de riesgos.
- Se genera un plan de implementación.

2.2.1.5. MEHARI

Método Armonizado de Análisis de Riesgos. Este método fue propuesto y desarrollado en 1996 por el Club Francés de la Seguridad de la Información (CLUSIF); todo tipo de organizaciones pueden acceder a él públicamente. Se actualiza continuamente para ayudar a los CISO a administrar las actividades de seguridad informática, pero también está pensada para auditores CIO o administradores de riesgos.

Este método es utilizado para apoyar a los responsables de la seguridad informática mediante un análisis riguroso de los factores principales de riesgo, evaluando de forma cuantitativa la situación de la organización acopla los nuevos métodos de funcionamiento de la

empresa con los objetivos estratégicos existentes mediante políticas de seguridad y mantenimiento de los riesgos [12].

Los aspectos básicos de esta metodología son: el diseño de un modelo de riesgo, la evaluación de la eficiencia de las políticas de seguridad que fueron propuestas previamente por la organización y la capacidad para evaluar y simular los niveles de riesgo. Con Mehari se puede analizar y razonar situaciones de riesgo además de detectar las vulnerabilidades mediante auditorías.

Mehari cuenta con tres módulos: análisis o evaluación de riesgos, evaluación de seguridad y análisis de amenazas, los cuales pueden ser seleccionados en base a las políticas y estrategias de la empresa a fin de decidir y construir planes de acción encaminados a mantener la seguridad de la información [12].

2.2.1.6. ISO/IEC 27005

Es una norma internacional que se ocupa de la gestión de riesgos de seguridad de la información. Este estándar proporciona una orientación para la gestión de riesgos de seguridad de la información de las empresas, esta norma es aplicable a todo tipo de organizaciones las cuales manejan información sobre organizaciones de riesgo que pueden complicar su seguridad [17].

Como se indicó al principio, el objetivo principal de esta norma es la gestión de los riesgos de seguridad de la información en una organización, mediante el uso de un enfoque específico para cada problema de seguridad de la información ya que una metodología no puede ser empleada en todos los problemas del Sistema de Gestión de Seguridad de la Información.

Hoy en día el estándar ISO/IEC 27005 se eliminará gradualmente después de la publicación del estándar ISO/IEC WD 27005 Information technology — Security techniques — Information security risk management, ya que este estándar será una modificación del estándar ISO/IEC 27005 [17].

2.2.1.7. CORAS

Consultative Objetive Risk Analysis System es un proyecto el cual fue desarrollado desde el año 2001 por Sintef, la misión de esta metodología es proporcionar un marco de trabajo para los sistemas críticos de seguridad. La ejecución de esta metodología permite la detección de vulnerabilidades, fallos, inconsistencias y redundancia que estén relacionados con la seguridad, esto se lo realiza mediante las siguientes etapas [18]:

- Presentación: Reunión inicial, para presentar los objetivos y el alcance del análisis y recolectar información para el inicio de la implementación.
- Análisis de alto nivel: Entrevistas para validar la información y documentación analizada para identificar amenazas, vulnerabilidades, escenarios e incidentes.
- Aprobación: Detalla los objetivos, alcance y consideraciones, para su aprobación.
- Identificación de riesgos: Identificación de amenazas, vulnerabilidades, escenarios e incidentes.
- Estimación de riesgo: Probabilidad e impacto de los incidentes identificados.
- Evaluación de riesgo: Emisión del informe de riesgos, para ajustes y correcciones.
- Tratamiento del riesgo: identificación de las salvaguardas y análisis coste/beneficio.

Esta técnica es muy útil para equipos heterogéneos que intenten identificar vulnerabilidades y amenazas a sus activos de valor. EL método Coras provee un editor gráfico en el que se diseñan y crean los modelos de lenguaje basados en Microsoft Visio, utiliza una librería de casos reutilizables, objetos de gestión de casos y formatos

generales de informes, lo cual facilita la comunicación entre diferentes partes del proceso de análisis de riesgo [18].

2.2.1.8. EBIOS

El nombre de esta metodología proviene de Expression des Besoins et Identification des Objectifs de Sécurités, es una metodología francesa la cual fue creada en 1995 y en la actualidad es mantenida por el ANSSI, este método se encarga de la gestión y análisis de los riesgos de seguridad en los sistemas de información, comprende un conjunto de guías y herramientas de código libre, enfocada a gestores del riesgo de TI [18]. Esta metodología se desarrolla mediante cinco fases:

- Fase 1: estudio del contexto
- Fase 2: estudio de los eventos peligrosos
- Fase 3: estudio de los escenarios de amenazas
- Fase 4: estudio de los riesgos
- Fase 5: estudio de las medidas de seguridad.

Esta metodología es una herramienta la cual está destinada principalmente a organizaciones gubernamentales y comerciales que trabajan con el Ministerio de Defensa. Permite evaluar y abordar los riesgos relacionados con la seguridad informática promoviendo una eficaz comunicación dentro de la organización y entre sus socios, dando cumplimiento a los últimos estándares de la ISO 27001, 27005 y 31000 para la gestión de riesgos y brindando las justificaciones necesarias para la toma de decisiones [18].

2.2.2. Comparativa de las Metodologías para la Gestión de Riesgos

Para realizar un correcto análisis de los riesgos para la empresa Ultralink se realizará una comparativa entre las diferentes metodologías que se pueden emplear como guía para la gestión de riesgos. Para realizar la comparativa se empleará una tabla en la cual se utilizarán los parámetros que se muestra a continuación

Tabla 3. Comparativa entre metodologías para la gestión de riesgos

Metodología	Ámbito de aplicación	Objetivos de seguridad	Ventajas	Desventajas
MAGERIT	Se la puede emplear en empresas grandes, PYMES, organismos de gobierno, compañías comerciales y no comerciales.	Cumple con todos los objetivos de seguridad.	• Permite realizar un análisis y gestión completa de los riesgos. • Es de carácter público por lo cual no requiere de autorización para su utilización. • Posee una buena base documental la cual está dividida en tres libros. • Posee herramientas para el análisis de riesgos como PILAR.	• No posee un inventario completo de las políticas. • No involucra a los procesos, recursos ni vulnerabilidades.
OCTAVE	Es empleable en PYMES, organizaciones privadas y públicas.	No cumple con los objetivos de trazabilidad y autenticidad.	• Se puede desarrollar por empleados que pertenecen a la organización. • Relaciona amenazas y vulnerabilidades. • Es una de las metodologías más completas ya que involucra a los procesos, recursos, amenazas, vulnerabilidades, activos y salvaguardas.	• No toma en cuenta el principio de no repudio de la información. • Para el análisis de los riesgos implementa mucha documentación. • Se debe poseer amplios conocimientos técnicos. • No se define de forma clara los activos de información.
NIST SP 800:30	Se utiliza en organizaciones gubernamentales y no gubernamentales.	No cumple con los objetivos de autenticidad y trazabilidad.	• Permite mejorar la administración de los resultados en el análisis de los riesgos. • Asegura los sistemas que se encarguen del	En la implementación de este modelo no se contempla la utilización d los procesos, las dependencias ni los activos.

			procesamiento, almacenamiento y transmisión de la información. • Bajo costo.	
CRAMM	Organizaciones públicas y privadas	No cumple con el objetivo de trazabilidad.	• Emplea un análisis de riesgos cuantitativo y cualitativo. • Permite realizar la clasificación de los activos de TI. • Combina el análisis y la evaluación de los riesgos. • Permite realizar una evaluación del impacto empresarial.	En este modelo no se contempla el uso de los recursos y los procesos.
MEHARI	Se lo utiliza en empresas medianas y grandes, compañías comerciales sin fines de lucro y en organizaciones de gobierno.	No toma en cuenta el objetivo de la autenticación de los usuarios.	• Emplea un análisis de riesgos cualitativo y cuantitativo. • Permite disminuir los riesgos dependiendo del tipo de organización. • Permite detectar vulnerabilidades mediante la utilización de auditorías. • Posee módulos separados para realizar una evaluación rápida o una evaluación detallada.	• No se incluye controles dentro de la gestión de los riesgos. • El proceso de gestión es complejo de manejar.
ISO/IEC 27005	Aplicable en cualquier organización.	No contempla los objetivos de autenticidad y trazabilidad.	• Es un estándar internacional por lo cual tiene una mayor aceptación.	• No posee técnicas ni herramientas que ayuden a su implementación. • No se pueden valorar las amenazas.

			• Posee un alcance completo en el análisis y gestión de los riesgos. • Permite realizar el monitoreo y revisión de los riesgos. • Es un complemento de la ISO 27001 y la ISO 27002.	
CORAS	Se lo emplea en sistemas de información se seguridad crítica	No contempla los objetivos de autenticidad y trazabilidad.	• Posee herramientas para el análisis de riesgos entre las cuales se destacan los editores gráficos. • Genera un reporte de las vulnerabilidades que se hallaron en la evaluación de los riesgos. • Se lo utiliza en el desarrollo y mantenimiento de nuevos sistemas.	• No realiza el análisis de riesgos de forma cuantitativa. • No utiliza los procesos y las dependencias.
EBIOS	Utilizado en el sector público, en pequeñas y grandes empresas del sector privado.	No contempla los objetivos de autenticidad y trazabilidad.	• Es una herramienta que permite la negociación y el arbitraje. • Es acoplable con la ISO27001: 2013,31000 y 27005. • Es una herramienta de código libre.	Se lo emplea como herramienta de soporte.

Fuente: [12] [19] [20]

2.2.3. Relación entre MAGERIT y la ISO/IEC 27001

Un sistema de seguridad de la información requiere de una metodología adecuada para su implementación, ya que de esta forma se realiza la evaluación de la información de una forma consistente. Al hablar sobre la gestión de seguridad de la información basados en la ISO 27001, se puede denominar a MAGERIT como el centro de todas las actividades ya que esta puede ser empleada en casi todas las etapas de la gestión de los riesgos. Entre las ventajas que se tiene al utilizar MAGERIT se tiene la realizar un análisis del impacto el cual nos permite identificar las amenazas y las vulnerabilidades a las cuales puede estar expuesta la seguridad de una empresa., otra de las ventajas es que es una metodología fácil de implementar ya que es una guía completa y detallada la cual permite llevar acabo un análisis de forma correcta también gracias a que esta alineada con los estándares que posee la ISO la implementación de esta metodología se puede tomar como punto de partida para mejorar los sistemas de gestión de información y su posterior certificación [21].

MAGERIT tiene una visión estratégica y global de la seguridad de los sistemas de información ISO 27001, esta visión comienza con un modelo de análisis y gestión de riesgos el cual está compuesto por los siguientes modelos: entidades, eventos y procesos. En cuanto a la tercera versión de MAGERIT posee un plan de entregas en el cual se puede observar cómo se encuentra el estado inicial y final deseado de la Seguridad del Sistema de Información según la ISO 27001, para delimitar el dominio y el rango de aplicabilidad según indica la ISO 27001 MAGERIT emplea diferentes técnicas las cuales pueden ser empleadas según el proyecto o la situación en la cual deba ser ejecutada [22].

2.2.4. Metodologías para la Gestión de Incidentes

El objetivo de la metodología de gestión de incidentes es reducir el impacto negativo de los incidentes en la organización y esto se logra restableciendo el servicio lo más pronto posible. Los incidentes pueden afectar a un usuario, a procesos completos o incluso a toda la

organización, por lo que es importante contar con un sistema eficaz para minimizar sus consecuencias.

Una metodología de gestión de incidencias bien implementado garantiza que los servicios no se vean interrumpido gracias a un correcto flujo de trabajo. Para que un servicio funcione de manera óptima se requiere una gestión eficaz de incidentes, capaz de solucionar cualquier inconveniente de forma eficaz, en el menor tiempo posible. Entre las metodologías de gestión de incidentes tenemos:

2.2.4.1. ITIL

Este método conocido por su abreviatura en ingles Information Technology Infrastructure Library, fue desarrollado en 1980 y ahora es el estándar de facto en la Gestión de Servicios de TI en todo el mundo. Esta metodología es una guía de buenas prácticas útil en todas las áreas de la organización [23].

El objetivo de ITIL es prevenir o recuperarse lo más rápido posible de cualquier interrupción o demora que afecte la calidad del servicio y reducir el impacto en las operaciones comerciales. La prioridad para este método es la velocidad de recuperación, eso significa que estos inconvenientes a menudo se resuelven mediante soluciones temporales en lugar de permanentes. En la actualidad ITIL se encuentra en la V4 y para poder gestionar los incidentes se debe seguir los siguientes pasos [24]:

- Detectar los incidentes
- Registrar los incidentes
- Categorización de los incidentes
- Priorización de los incidentes
- Resolución de los incidentes

La gestión de incidencias no finaliza con el cierre de este, ya que uno de los enfoques de ITIL4 es la mejora continua, buscando

constantemente soluciones preventivas para evitar que surjan problemas los cuales traten de afectar la calidad del servicio.

2.2.4.2. NIST 800-61

Es un documento fue publicado por el Instituto de Estándares Y Tecnologías (NIST), está conformado por 4 capítulos y 9 apéndices, esta guía ayuda a las organizaciones a establecer una manera eficiente de respuesta y manejo de incidentes de seguridad informática. Esta guía proporciona pautas para la gestión de incidentes, también proporciona un análisis sobre los datos relacionados con los incidentes por lo cual se puede determinar la respuesta más apropiada para cada tipo de incidente. Las pautas se pueden seguir independientemente de las plataformas de hardware, protocolos, sistema operativo o aplicaciones utilizadas [25].

2.2.4.3. ISO 27035

La ISO 27035 es una guía para evaluar y analizar las vulnerabilidades e incidentes a los que una organización puede estar expuesta. Este enfoque de mejores prácticas de gestión de incidentes puede ser implementado en organizaciones pequeñas, medianas y grandes [26].

La gestión de incidentes permite generar controles de detección y correctivos los cuales ayudan a minimizar los impactos. La guía proporciona un enfoque estructurado para:

- Identificar, comunicar y evaluar los incidentes de la seguridad.
- Gestionar y responder ante los incidentes de la seguridad de la información.
- Examinar, identificar y gestionar las vulnerabilidades de seguridad.
- Promover la mejora continua de la seguridad de la información y de la gestión de incidentes.

ISO-27035 es un proceso que está conformado por cinco etapas las cuales son:

- Preparación para el enfrentamiento ante incidentes.
- Registro de incidentes de seguridad.
- Inspección de los incidentes y la posterior elección de la decisión sobre cómo hacer las cosas.
- Investigar y resolver los incidentes.
- Aprender de las lecciones.

CAPITULO III SITUACIÓN ACTUAL DE LA EMPRESA

3.1. Antecedentes de la empresa

Ultralink es una empresa creada en el 2009 cuya finalidad es brindar servicios de telecomunicaciones y conectividad a través de redes e infraestructura moderna, cumpliendo la normativa vigente e impulsando el crecimiento económico de nuestro país; logrando que todos los habitantes, puedan acceder al servicio de datos e internet bajo la premisa de calidad y precio asequible [27].

Figura 7.Logo de la Empresa

Fuente: https://ultralink.ec/

El objetivo de Ultralink es posicionar a la empresa como un referente en el servicio de internet, prestando un buen servicio con lo cual se garantiza el menor retardo en la navegación.

Cuenta con una red de respaldo la cual garantiza un tiempo de actividad mayor al que su competencia presenta en Ecuador. A partir del año 2018 busca proveer a sus clientes mejor acceso a tecnologías de la información mediante la incorporación de infraestructura de fibra óptica GPON /FTTH. También brinda servicios integrales en Telecomunicaciones y Tecnologías de la Información, soportados por personal altamente calificado. [27]

3.2. Misión

Generar valor a la sociedad y a todos los grupos de interés, mediante una gestión eficiente, innovadora y de calidad en la prestación de servicios de telecomunicaciones, a través del compromiso y experiencia de nuestro equipo de colaboradores [27].

3.3. Visión

Ser una empresa líder en los servicios integrales de Telecomunicaciones, contribuyendo de forma positiva a la sociedad [27].

3.4. Organigrama de la empresa

Luego de las entrevistas que se llevaron a cabo con los representantes de la empresa se facilitó el siguiente organigrama que se muestra a continuación.

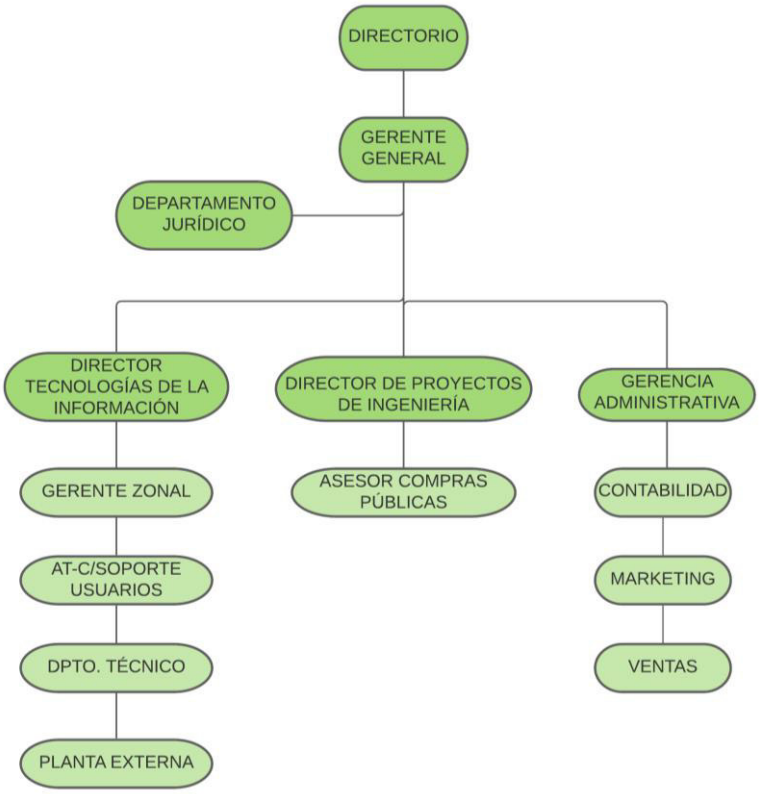


Figura 8. Organigrama de la empresa Ultralink

Fuente: Autores del Proyecto

3.5. Departamentos

La empresa Ultralink se encuentra conformada por los departamentos que se muestran en la Figura 9 y los cuales se los detallara a continuación:

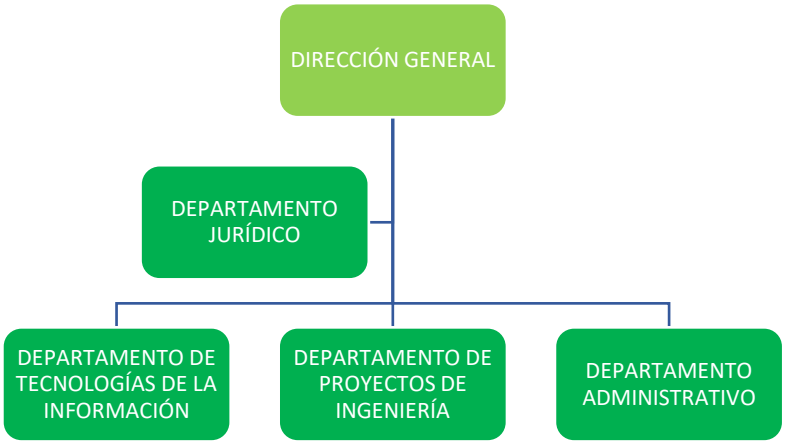


Figura 9. Departamentos de la empresa Ultralink

Fuente: Autores del Proyecto

- **Dirección General:** Es el departamento que se encarga de la toma de decisiones de la empresa siempre tomando en cuenta los objetivos de la empresa.
- **Departamento Jurídico:** La finalidad de este departamento es atender todos los asuntos legales de la empresa tanto los asuntos internos como externos.
- **Departamento de Tecnologías de la Información:** Es el departamento encargado de la correcta administración de los recursos tecnológicos que posee la empresa.
- **Departamento de Proyectos de Ingeniería:** La finalidad que posee este departamento es la de asesorar y gestionar las compras que realiza la empresa.
- **Departamento Administrativo:** En este departamento se encuentra la contabilidad, el marketing y las ventas por lo cual las funciones que se desarrollan tratan sobre el registro de los cambios económicos que se generan en la empresa día a día, investigación de mercado, planificación de estrategias de marketing, etc.

3.6. Estado actual de la seguridad

Para comprender el estado actual de la seguridad en la organización se procedió a realizar un diagnóstico con el objetivo de poder saber la situación que presenta la entidad frente a la implementación de un Sistema de Gestión

de Seguridad de la Información basado en la norma ISO/IEC 27001:2013. En términos generales se pudo identificar las siguientes situaciones:

- Falta de conocimiento sobre los temas de seguridad por parte de los funcionarios de la empresa.
- Falta de cooperación de la Gerencia en los procesos de seguridad de la empresa.
- La no existencia de controles de seguridad tanto físicos como virtuales.
- No se posee políticas de seguridad ya que estas aún no han sido creadas.
- Falta de departamentos que estén encargados de la seguridad de los activos de información tanto físicos como digitales.
- No se realizan capacitaciones al personal sobre los riesgos de seguridad.

3.6.1. Estratificación de la empresa

La identificación del nivel al cual pertenece una empresa nos permite identificar, el nivel de complejidad que puede tener la empresa al momento de implementar un Sistema de Gestión de Seguridad de la Información.

Para poder dividir a las organizaciones existen muchas maneras de catalogarlas: desde su conformación jurídica, sector de actividad o incluso si es pública o privada, pero una de las formas más comunes de clasificar a las organizaciones es de acuerdo con su tamaño [28]. Según el Directorio de Empresas y Establecimientos (DIEE) en Ecuador la clasificación de las empresas dependiendo su tamaño muestra que en 2019 las empresas están clasificadas en empresas medianas, empresas grandes y microempresas, así como se observa en la Figura 10.

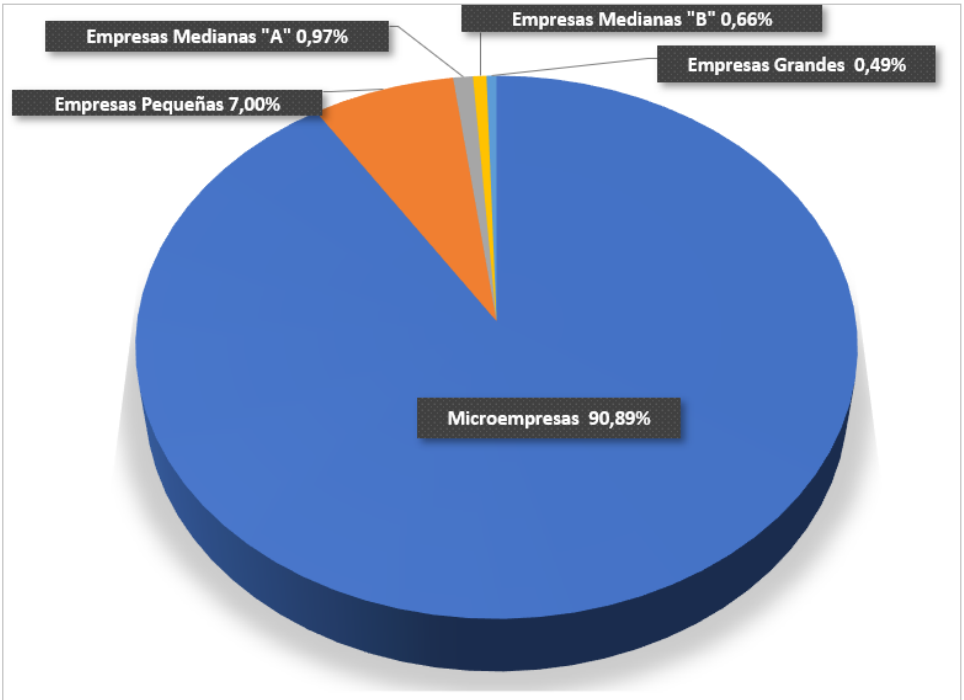


Figura 10.Distribución del número de empresas

Fuente: Autores del Proyecto

Con los datos que se observa en la gráfica se puede mirar que la mayoría de las empresas en el país son microempresas las cuales no poseen los recursos necesarios para la implementación de un SGSI, lo cual es un gran inconveniente para la seguridad de estas.

Otra forma de organizar a las empresas presentes según sus dimensiones Ecuador emplea la definición que proporciona la Comunidad Andina de Naciones (CAN) por lo cual las empresas en nuestro país quedan divididas de la siguiente manera [28].

Tabla 4. Clasificación de las empresas

Tipo de empresa		**# de empleados**	**Valor bruto en ventas anuales**	**Activos**	**Característica**
Microempresa		De 1 a 9	Igual o menor a 100.000	Hasta 100.000	Este tipo de negocio es el más pequeño en tamaño, generalmente son los negocios familiares o emprendimientos.
PYMES	Pequeña	De 10 a 49	Desde 100.001 a 1.000.000	Desde 100.001	Son más grandes que una microempresa. Tiene una división de

				hasta 750.000	funciones y una mejor organización de los recursos.
	Mediana	De 50 a 199	Desde 1.000.000 a 5.000.000	Desde 750.001 hasta 3.999.000	Se trata de empresas que habitualmente se dedican a la creación de productos o a prestar servicios comerciales e industriales
Gran empresa		Más de 200	Más de 5.000.000	Más de 4.000.000	Son las corporaciones con un gran poder en el mercado, las cuales generalmente son multinacionales.

Fuente: Autores del Proyecto

3.6.2. Niveles de cumplimiento de la ISO 27001: 2013 en Ultralink

Por medio de un análisis que se realizó al Anexo 2 y Anexo 3, se logró realizar el análisis del nivel de cumplimiento que posee la entidad en relación con los objetivos de control (Anexo 2) y controles definidos en el (Anexo 3) de la norma ISO/IEC 27001: 2013, con estos resultados se posee una idea más clara para poder implementar las fases de un SGSI en la empresa

Para realizar este diagnóstico se utilizó modelos de niveles de madurez para determinar la existencia o falta de implementación de los controles que comprende la ISO 27001: 2013. Tomaremos en cuenta la numeración del 0 al 5 siendo 0 la no existencia y 5 la opción optimizada, los modelos que se utilizaron fueron respondidos por funcionarios del área de Tecnología ya que los controles de la norma ISO/IEC 27001: 2013 están orientados a proteger la seguridad de las personas, de la infraestructura física y lógica, de los recursos tecnológicos y por ende de la información. En base a la información recopilada en los anexos antes mencionados se obtiene los siguientes gráficos.

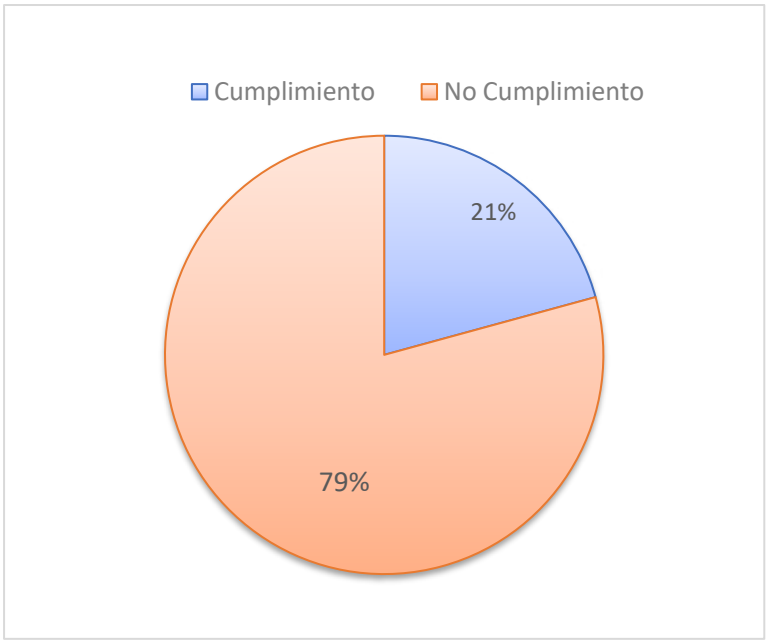


Figura 11. Nivel de cumplimiento controles Anexo A ISO 27001: 2013

Fuente: Autores del proyecto

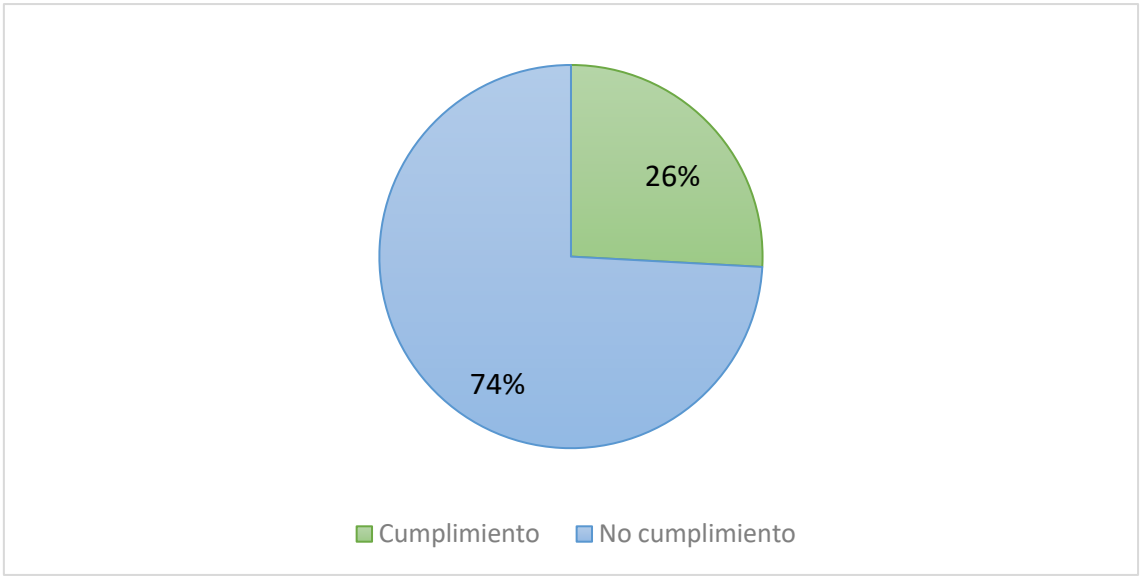


Figura 12. Niveles de cumplimiento de controles Anexo A ISO 27001: 2013

Fuente: Autores del proyecto

Según los resultados sobre los niveles de cumplimiento de los controles establecidos en el Anexo 2 y Anexo 3 de la norma ISO/IEC 27001: 2013, la empresa debe crear los controles y reforzar los existentes ya que estos en muchos casos poseen un bajo grado de cumplimiento. Para cumplir con lo antes mencionado se debe mejorar los mecanismos

y herramientas tecnológicas existentes. El nivel de cumplimiento de los controles de los Anexo 2 y 3 de la ISO 27001: 2013 también nos indica el grado de madures que posee la empresa en la protección de sus activos de información y la gestión de la seguridad de la información tomando en cuenta los niveles de riesgos y las normativas vigentes relacionadas a la seguridad.

Para determinar el nivel de riesgos que posee la empresa nos basaremos en el nivel de cumplimiento de los controles mediante la clasificación de Bajo, Medio y Alto, así como se muestra en la Tabla 4:

Tabla 5. Nivel de cumplimiento vs Nivel de riesgos

Nivel de Cumplimiento	Nivel de Riesgo	Implicaciones
Alto	Bajo	Los controles de seguridad que posee la empresa son óptimos lo cual nos demuestra que se posee un nivel apropiado de protección de los activos de información y una madures en la seguridad de la información.
Medio	Medio	La empresa posee algunos controles implementados, pero estos están sin documentar o están implementados de forma incorrecta, por lo cual requieren una revisión y de esta forma mejorar su eficiencia y su cumplimiento. Esta situación representa debilidades en algunos de los controles las cuales pueden ser aprovechadas por las amenazas.
Bajo	Alto	Un nivel bajo de cumplimiento o la ausencia de controles representa un inadecuado nivel de protección de los activos de información y un incumplimiento de la normativa de seguridad de la información. Para este caso se debe implementar urgentemente medidas de seguridad con el objetivo de disminuir las brechas encontradas.

Fuente: Autores del Proyecto

El análisis del nivel de cumplimiento de la empresa frente a los niveles de riesgos es BAJO ya que la mayoría de los controles poseen un nivel de cumplimiento menor al 33% lo que implica que no tiene la implementación de los controles y objetivos de control de los requerimientos establecidos en la ISO 27001: 2013, por lo que la empresa no posee controles aptos para el cuidado los activos de

información. En el siguiente gráfico se presenta el resultado de cada uno de los objetivos de control que se analizó en los Anexo 3.

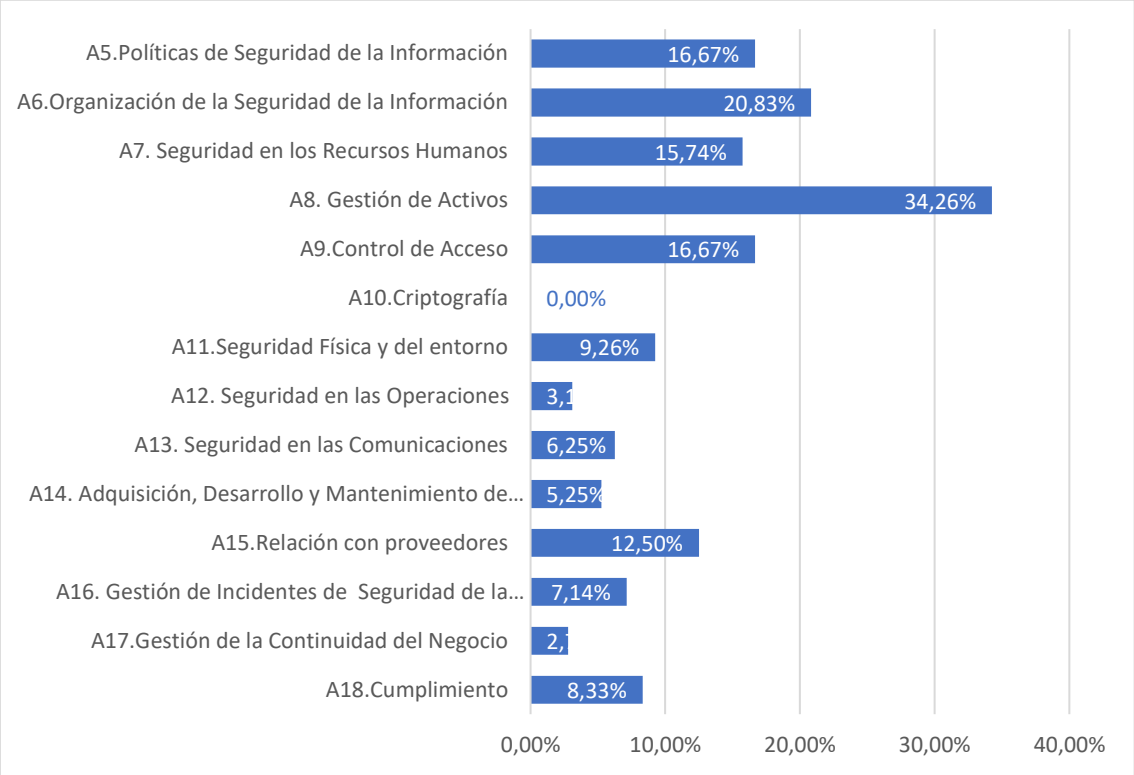


Figura 13. Nivel de cumplimiento de los dominios de control

Fuente: Autores del Proyecto

3.6.2.1. Objetivos de control de nivel de cumplimiento BAJO

Son los objetivos de control que posee la empresa que se encuentra en un grado BAJO de cumplimiento es decir menor o igual al 33%. Los controles que poseen este nivel representan un riesgo ALTO para la empresa ya que existe una inadecuada implementación o la inexistencia de estos, no se cumple con las normativas de seguridad de la información y no se posee una correcta protección de los activos de la información. A continuación, se muestra cuáles son objetivos de control que se encuentran en este nivel.

Tabla 6. Objetivos de control con nivel BAJO de cumplimiento

Objetivo de control	**% Cumplimiento**
A10.Criptografía	0,00%
A17.Gestión de la Continuidad del Negocio	2,78%
A12. Seguridad en las Operaciones	3,10%
A14. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	5,25%

A13. Seguridad en las Comunicaciones	6,25%
A16. Gestión de Incidentes de Seguridad de la Información	7,14%
A18.Cumplimiento	8,33%
A11.Seguridad Física y del entorno	9,26%
A15.Relación con proveedores	12,50%
A7. Seguridad en los Recursos Humanos	15,74%
A9. Control de Acceso	16,67%
A5. Políticas de Seguridad de la Información	16,67%
A6. Organización de la Seguridad de la Información	20,83%

Fuente: Autores del proyecto

3.6.2.2. Objetivos de control de nivel de cumplimiento MEDIO

Son los objetivos de control que posee la empresa que se encuentra en un grado MEDIO de cumplimiento es decir mayor al 33% y menor al 77%. Los controles que poseen este nivel representan un riesgo MEDIO para la empresa ya que estos controles están documentados de forma inadecuada o presentan debilidades las cuales pueden causar la materialización de las amenazas. A continuación, se muestra cuáles son objetivos de control que se encuentran en este nivel.

Tabla 7. Objetivos de control con nivel MEDIO de cumplimiento.

Objetivo de control	% Cumplimiento
A8. Gestión de Activos	34,26%

Fuente: Autores del proyecto

3.7. Normativas de seguridad aplicables en Ecuador

Son las normativas que regulan los procedimientos que deben emplear las empresas ecuatorianas para proteger sus activos tanto físicos como informáticos. A continuación, se muestra las normativas que se debe tener en cuenta.

3.7.1. Ley de Comercio Electrónico, Firmas y Mensajes de Datos

Es la ley que permite regular los servicios de contratación electrónica, la firma electrónica, la prestación de servicios electrónicos, la protección a los usuarios que empleen los servicios electrónicos y los mensajes de datos mediante. Esta regulación se realiza mediante el uso de redes de información [29].

3.7.2. Ley Orgánica de Protección de Datos Personales

Esta ley tiene como objetivo garantizar el derecho a la protección de los datos personales, esto incluye el acceso, eliminación y disposición de la información, así como la protección de esta. Esta ley fue creada por la asamblea nacional en el 2021 [30].

3.7.3. Código Orgánico Integral Penal

La finalidad de este Código es normar el poder penal que posee el Estado mediante la tipificación de las infracciones penales, el establecimiento de procedimientos para el juzgamiento de las personas, fomentar la rehabilitación social de las personas que han sido sentenciadas y la reparación integral de las víctimas [31].

CAPITULO IV DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1. Consideraciones Iniciales

4.1.1. Partes interesadas de la empresa

Las partes interesadas de la empresa son las personas naturales o jurídicas que interactúan en el ejercicio de sus funciones, estas pueden afectar de manera positiva o negativa a la seguridad de la información.

En la tabla se podrá observar las partes interesadas de la empresa en función a la seguridad de la información.

Tabla 8. Partes interesadas internas en función del SGSI

Partes interesadas	Descripción
Alta Directiva	Son los encargados de liderar la empresa y salvaguardar la información para de este modo cumplir con los objetivos estratégicos de la organización
Dirección de Tecnología	Son los individuos encargados de todos los aspectos relacionados con la continuidad de la tecnología y la seguridad de la información en la empresa
Gestión humana	Son los encargados de realizar la capacitación antes y después de la vinculación de los funcionarios
Colaboradores	Son los encargados de los activos que posee la empresa

Fuente: Autores del proyecto

Tabla 9. Partes interesadas externas en función del SGSI

Partes interesadas	Descripción
Accionistas	Son la personas jurídicas o naturales que poseen acciones de la empresa
Gobierno	Es un grupo de individuos que poseen la potestad para generar normativas de funcionamiento de la empresa.
Entes de control externo	Son los entes que se encargan de controlar y vigilar las actividades que desarrolla la empresa
Proveedores	Son las personas naturales o jurídicas las cuales prestan sus servicios a la empresa
Comunidad	Son los grupos externos o individuos que se ven beneficiados por las actividades desarrolladas por la entidad

Fuente: Autores del proyecto

4.1.2. Recursos disponibles

Son los recursos que se poseen para el diseño del SGSI, entre estos tenemos los siguientes:

- **Metodologías:** Son las guías que permiten la generación del SGSI tomando en cuenta la gestión de los incidentes y riesgos.
- **Apoyo de la organización:** Son todas las acciones que ayudan a la ejecución del presente trabajo de titulación.
- **Información:** Son aquellos datos suministrados por la empresa para el desarrollo del presente trabajo entre estos datos tenemos:
    - Información sobre los activos que posee la organización.
    - Información sobre las amenazas a las cuales pueden estar expuestas los activos que posee la empresa.
    - Información sobre las vulnerabilidades que posee la institución.

4.2. Metodología para la Gestión de Riesgos

Luego de realizar el análisis comparativo de las diferentes metodologías existentes para la gestión de riesgos y tomando en cuenta los criterios mostrados en la Tabla 3 se llegó a la conclusión que para el caso de estudio presente en este trabajo la mejor opción es MAGERIT la cual nos permite generar y determinar las medidas apropiadas para dar un tratamiento adecuado a los activos que posee la empresa y de esta forma realizar un correcto análisis de los riesgos.

4.3. Identificación y Valoración de los Activos

4.3.1. Identificación y clasificación de activos

Para la identificación de los activos que posee la empresa Ultralink se realizó un inventario el cual se lo desarrollo con la ayuda del personal del departamento de tecnología los cuales proporcionaron la información y los recursos necesarios. El formato que se utilizó para el inventario es el que se muestra en la Tabla 10 en la cual se incluye un ejemplo de un activo registrado. Para poder observar todo el inventario de los activos se lo puede realizar en el Anexo 5.

Tabla 10. Inventario de activos

COD	Área	Equipo	Detalles del Equipo				Ubicación	Responsable	Características	Custodio
			Marca	Modelo	Procesador	Memoria				
01	Departamento técnico	Laptop	ASUS	X441UAK	I7 7500U	4 GIGAS	Departamento técnico	Departamento técnico	Windows 10 pro de 64 bits	Víctor Erazo

Fuente: Autores del Proyecto

Para la clasificación de los activos en un sistema informático hay dos valores esenciales los cuales son la información que se maneja y los servicios que se prestan [32]. De los activos antes mencionados se tomó en cuenta las siguientes categorías:

- Hardware: Son todos los elementos físicos que posee la empresa y estos son empleados en los diferentes servicios que oferta la empresa.
- Software: Son los programas que utiliza la empresa para los diferentes servicios que brinda la empresa.
- Personal: Son todos los individuos que trabajan en el sistema de información que posee la empresa.
- Información: Es el activo más valioso de la empresa sin el cual no podría trabajar la empresa.
- Servicios: Son aquellas actividades que proporciona la empresa para satisfacer necesidades.
- Las instalaciones: Son aquellas que acogen los equipos informáticos.
- Equipamiento auxiliar: Son los dispositivos utilizados para dar soporte a los equipos principales que posee la infraestructura informática.

A continuación, se muestra la tabla de la clasificación de los activos que posee la empresa según las clasificaciones antes mencionadas.

Tabla 11. Clasificación de los activos

Clasificación	Activos
Hardware	• Equipos de escritorio • Laptops • Servidores • Routers

	• Switch

Software	• Software de manejo de red
	• Sistema contable trantor
	• Sistemas operativos
	  ○ Windows
	  ○ Ubuntu
	• Office 2010
	• Máquinas virtuales

Personal	• Personal interno • Proveedores
Información	• Información de contratación • Bases de datos • Planillas de pagos • Contratos de servicios • Documentos compartidos • Ordenes de trabajo • Información de servicios • Diagrama de red
Servicios	• Correo electrónico
Instalaciones	• Edificios • Vehículos terrestres
Equipos auxiliares	• UPS • Equipos de climatización • Suministros esenciales

Fuente: Autores del Proyecto

4.3.2. Valoración de los activos

La valoración de los activos es la acción mediante la cual se otorga un valor al activo sea de forma cualitativa o cuantitativa. Tomando en cuenta algunas de las dimensiones de valoración que posee MAGERIT se puede realizar un análisis de riesgos. Para obtener esta valoración se realizó encuestas al personal que está involucrado directamente con los activos y de esta forma obtener los datos correctos para la ejecución del análisis. Las dimensiones que se tomaron en cuenta al momento de realizar las encuetas son:

- Confidencialidad
- Integridad
- Disponibilidad

4.3.2.1. Criterios de valoración

Según MAGERIT se puede implementar cualquier escala de valoración, pero hay que tomar en cuenta las siguientes condiciones [33]:

- Se debe utilizar una escala en común para todas las dimensiones a ser analizadas.
- Los criterios para realizar la evaluación deben ser homogéneos ya que de esta manera se puede realizar una comparación de los analices que se ejecuta de forma separada.

Con lo antes expuesto se eligió una escala la cual consta desde el valor 0 al valor 5 los cuales tienen una valoración de despreciable y extremo respectivamente. A continuación, se muestra en la Tabla 12 los valores que poseen cada uno de los valores en la escala [33].

Tabla 12. Criterios de valoración

Valor		**Criterio**
5	Extremo	Daño extremadamente grave
4	Muy alto	Daño muy grave
3	Alto	Daño grave
2	Medio	Daño importante
1	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: [33]

Teniendo en cuenta la tabla anterior y los criterios de confidencialidad, integridad y disponibilidad se procedió a realizar la valoración de los activos para lo cual se realizó el promedio de las tres dimensiones antes mencionadas En la Tabla 13 se muestra un ejemplo de esta valoración y el resto de los datos se encuentran en el Anexo 6.

Tabla 13. Valoración de los activos

Nombre del Activo	**Ubicación**	**Valoración de la pérdida del activo**			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
Laptop Asus	Departamento técnico	2	4	2	3
Laptop DELL	Departamento técnico	2	4	2	3
Laptop	Departamento administrativo	3	4	3	3
DELL NUC Asus	Departamento administrativo	3	4	3	3
Pc Escritorio	Gerencia	3	3	3	3

Fuente: Autores del Proyecto

4.4. Identificación de Vulnerabilidades y Amenazas

La identificación de las amenazas y las vulnerabilidades se lo realizó utilizando la información proporcionada por los custodios de los activos y el catalogó de amenazas y vulnerabilidades que nos proporciona MAGERIT. A continuación, se muestra las amenazas y las vulnerabilidades a las cuales están expuestos los activos que posee la empresa.

Tabla 14. Identificación de las Vulnerabilidades y Amenazas

Activo	Vulnerabilidades	Amenazas
Hardware	Falta de mantenimiento en el sistema antiincendios	Incendio
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos Error en la manipulación
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo
	No existe control sobre las personas que ingresan y salen de la organización	Robo
	Falta de conexiones seguras	Error en la manipulación de las redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total
Software	Errores en la configuración de seguridad	Ciberataques
	Asignación errada en los accesos	Abuso de los equipos
	Ausencia de documentación de uso	Modificación sin autorización
	Inadecuada utilización de los sistemas	Errores de mantenimiento
	Interfaces de difícil manipulación	Errores de uso
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos
	No existencia de copias de seguridad	Mal funcionamiento del software
Personal	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos

	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos
	Entrenamiento insuficiente del personal	Perdida de personal clave
	No existencia de políticas de mensajería	Perdida de los datos
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso
Información	Inadecuada administración de los datos	Fuga de información
	Falta de protecciones físicas adecuadas	Daños por agua o fuego
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos
	Falta de plan de continuidad del negocio	Contratos de forma incompleta
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres Naturales
	No existencia de copias de respaldo	Perdida de información
Instalaciones	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado
	Ausencia de protecciones digitales	Perdida de equipos
	Ubicación en área susceptible a desastres	Desastres Naturales
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía
	Perdida de información	Destrucción de los equipos
Equipos auxiliares	Falta de mantenimiento en el sistema antiincendios	Incendio
	No se posee sistema de refrigeración actual	Fallos en los equipos
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos
	Monitoreo inadecuado de las instalaciones	Robo
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión

Fuente: Autores del Proyecto

4.4.1. Valoración de las Amenazas

Una vez que se ha determinado tanto las amenazas como las vulnerabilidades a las cuales pueden estar expuestos los activos que posee la empresa se procedió a realizar la valoración tomando como base

una escala la cual estará compuesta por desde del 0 hasta el 5 siendo despreciable y extremo respectivamente. Ya que cada activo está expuesto a diferentes amenazas y vulnerabilidades para esta valoración se toma en cuenta la probabilidad y la frecuencia de la ocurrencia,

Tabla 15. Criterios de valoración de las Amenazas

Valor	Degradación	Probabilidad de ocurrencia
5	Muy alta	Daño diario
4	Alta	Daños mensuales
3	Media	Mas de una vez al año
2	Baja	Una vez al año
1	Muy Bajo	Rara vez
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Autores del Proyecto

Una vez que ya se determinaron las dimensiones que se van a tomar en cuenta se procedió a generar un check-list, así como se muestra en el ejemplo que se presenta en la Tabla 16ya que el resto de los datos se encuentran en el Anexo 7.

Tabla 16. Matriz de evaluación de Amenazas

Activo	Vulnerabilidades	Amenazas	Degradación	Probabilidad de la ocurrencia	Justificación
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos Error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas	Robo	2	2	No se controla las personas que pude

	que ingresan y salen de la organización				ingresar a la organización

Fuente: Autores del Proyecto

4.5. Controles Existentes

Anteriormente en el capítulo tres se indicó la situación de la seguridad en la cual se encuentra la empresa, en la cual se pudo observar que las medidas de control que la empresa posee son muy bajas y los planes para tratar los riesgos están en procesos de implementación o no se los posee por lo cual las amenazas pueden materializarse de forma más eminente y efectiva. A continuación, en la Tabla 17 se muestra los controles existentes en la empresa los cuales son utilizados por la misma para proteger sus activos ante las amenazas que pueden atentar a la seguridad.

Tabla 17. Controles existentes en Ultralink

Amenazas	**Controles implementados**
Amenazas ambientales y físicas	• Extintores, alarmas de humo • Sistemas de climatización • Sistemas de suministro de energía UPS
Técnicas	• Personal capacitado
Humanas o accidentales	• Documentación y capacitación sobre el uso de las herramientas • Firewall • Antivirus • Procedimientos para la selección y contratación del personal
Organizacionales	• Licencias adquiridas para brindar los servicios • Garantías

Fuente: Autores del Proyecto

4.6. Evaluación de Riesgos

Una vez que se ha identificado a los activos y se ha determinado la importancia de estos se procedió a valorar las vulnerabilidades y amenazas que pueden afectarlos. Con los valores obtenidos en los procesos antes mencionados se procedió a calcular el riesgo para lo cual se debe tener en cuenta los criterios que se muestran a continuación:

4.6.1. Impacto

El impacto se lo podría definir como el daño que sufre un activo al materializarse las amenazas, para determinar este daño se debe tener en

cuanta como son afectadas las dimensiones de confidencialidad, integridad y disponibilidad que posee cada uno de los activos. Para poder asignar un valor de forma cuantitativa a cada una de las dimensiones antes mencionadas se tomó en cuenta la escala del 1 al 5 así como se muestra en la siguiente tabla.

Tabla 18. Criterios de valoración del impacto

Valor	Magnitud del impacto	Escala	Descripción
5	Muy alto	MA	Cuando se materializa las amenazas generan grandes impactos en los activos de la organización
4	Alto	A	Cuando se materializa la amenaza se generan altas consecuencias en los activos
3	Medio	M	Cuando se materializa la amenaza se generan consecuencias medias en los activos
2	Bajo	B	Cuando se materializa la amenaza y se generan consecuencias bajas en los activos
1	Muy bajo	MB	Cuando se materializa la amenaza y se generan mínimas consecuencias en los activos
0	Despreciable	D	Cuando se materializa la amenaza, pero no tiene afectaciones en la organización

Fuente: Autores del Proyecto

Una vez que se ha definido la valoración que tiene cada uno de los activos se pudo obtener el grado de afectación que generaría la materialización de las amenazas a los activos que posee la empresa. En la tabla que se encuentra a continuación se muestra un ejemplo de los valores obtenidos en las dimensiones analizadas tomando en cuenta los criterios de confidencialidad, integridad y disponibilidad y de esta forma determinar el impacto que se generaría en los activos. Para observar la valoración total del impacto en los activos revisar el Anexo 8.

Tabla 19. Matriz de valoración del impacto de las amenazas en función de CID

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del impacto CID			Valor total del impacto CID	Impacto	Magnitud del impacto			Magnitud total del impacto
			C	I	D			C	I	D	

Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	4	9	3	B	M	A	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	4	4	10	3	B	A	A	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	4	5	13	4	A	A	MA	A
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	1	2	5	2	B	MB	B	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	1	1	3	5	2	MB	MB	M	MB

Fuente: Autores del Proyecto

4.6.2. Probabilidad de ocurrencia

Para determinar la probabilidad se debe tener en cuenta la facilidad con las que se pueden generar las amenazas a partir de las vulnerabilidades existentes en la empresa. En un sistema de información se pueden generar diferentes tipos de amenazas por lo cual la probabilidad de que estas se generen es diferente. Los criterios que se emplean son una escala de 5 valores los cuales van desde el numero 1 al 5 con sus respectivos criterios.

Tabla 20. Matriz de análisis de probabilidad de ocurrencia

Valor	Escala	Probabilidad	Degradación
5	MA	Muy probable	Muy alta
4	A	Probable	Alta
3	M	Posible	Media
2	B	Poco Posible	Baja
1	MB	Muy Raro	Muy Bajo
0	D	Despreciable	Irrelevante en la práctica

Fuente: [33]

Una vez definidos los criterios con los cuales se va a realizar el cálculo de la probabilidad de ocurrencia se procedió a valorar los activos de la forma que se muestra en la tabla que está a continuación. Para poder observar la valoración de todos los activos que posee la empresa se debe revisar el Anexo 9 ya que los datos que se encuentran en la parte de abajo son solo un ejemplo de los datos totales que se generó.

Tabla 21. Matriz de valoración de probabilidad de ocurrencia

Nombre del Activo	Vulnerabilidades	Amenazas	Valoración		Valoración total de la probabilidad	Probabilidad de ocurrencia	Magnitud		Magnitud total de la probabilidad
			Degradación	Probabilidad			Degradación	Probabilidad	
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B

Fuente: Autores del Proyecto

4.6.3. Riesgo estimado

Para poder obtener el riesgo estimado se procede a multiplicar el impacto por la probabilidad de ocurrencia este nuevo valor que se obtiene se lo conoce como el riesgo efectivo. El cálculo antes descrito se lo empleará para realizar la evaluación y tratamiento de los riesgos, también para se

empleará los criterios que se muestran en la Tabla 22 los cuales están ubicados según su prioridad.

Tabla 22. Criterios de evaluación de riesgos

Escala	Nivel	Criterio	Descripción
20-25	MA	Muy alto	El riesgo que se genera es extremo. Su ocurrencia implicaría una pérdida total de la información
15-19	A	Alto	El riesgo es alto ya que la probabilidad de ocurrencia e impacto son altos. La ocurrencia de este tipo de riesgos implica una perdida alta de la información
10-14	M	Moderado	El riesgo es alto ya que la probabilidad de ocurrencia e impacto son altos. La ocurrencia de este tipo de riesgos implica una perdida alta de la información
5-9	B	Bajo	El riesgo es bajo ya que la probabilidad de ocurrencia e impacto son bajos. La ocurrencia de este riesgo implica una perdida baja de la información
1-4	MB	Muy bajo	El riesgo es leve ya que la probabilidad de ocurrencia e impacto son muy bajos. La ocurrencia de este riesgo implica una perdida casi nula de la información

Fuente: [34]

Luego de haber definido los criterios con los cuales se va a realizar la valoración del riesgo se logró obtener el nivel de riesgo al cual está expuesto cada activo que posee la empresa, a continuación, se muestra en la Tabla 23 un ejemplo de cómo se obtuvieron estos valores. Para poder observar la valoración de todos los activos que posee la empresa se debe revisar el Anexo 10.

Tabla 23. Matriz del cálculo del riesgo

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Magnitud del impacto	Valor de la probabilidad de ocurrencia	Magnitud de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	3	M	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B

	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	A	1	MB	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	B	3	M	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	B	2	B	4	MB

Fuete: Autores del Proyecto

4.6.4. Matriz de calor

La matriz de calor nos permite representar de forma gráfica las zonas en las cuales se encuentran los riesgos de acuerdo con su impacto y probabilidad de ocurrencia. Cada una de las zonas dentro de esta matriz de calor corresponde a un tipo de riesgo por lo cual en la Tabla 24 se definió la siguiente gama de colores dependiendo de la puntuación, el criterio de cada riesgo y las acciones que se deben realizar.

Tabla 24. Gama de colores para la matriz de calor

Escala	Nivel	Criterio	Acciones
20-25	MA	**Muy alto**	Se requiere acciones inmediatas las cuales permitan reducir, compartir o transferir el riesgo
15-19	A	**Alto**	Se requiere de una atención urgente y una implementación de medidas las cuales ayuden a reducir el nivel del riesgo
10-14	M	**Moderado**	Se requiere implementar medidas lo más pronto posible las cuales permitan disminuir el riesgo a un nivel bajo o muy bajo
5-9	B	**Bajo**	Se debe implementar medidas preventivas las cuales ayudan a prevenir y reducir el riesgo
1-4	MB	**Muy bajo**	Se puede tolerar este tipo de riesgo ya que no es necesario tomar medidas de control diferentes a las ya existentes

Fuente: [35]

Una vez definidos los colores de la matriz se procedió a la creación de la matriz de 5x5 en la cual se especifica el puntaje que posee el tipo de riesgo, la zona a la cual pertenece y las acciones que se debe desarrollar para el tratamiento del riesgo.

Tabla 25. Matriz de calor

Impacto		Probabilidad				
		MB	B	M	A	MA
		1	2	3	4	5
MA	5	5 puntos Zona de riesgo bajo Administrar el riesgo	10 puntos Zona de riesgo moderado Reducir el riesgo a niveles más bajos	15 puntos Zona de riesgo alto Evitar la gestión de los riesgos	20 puntos Zona de riesgo muy alto Evitar- gestionar el riesgo Requiere acción inmediata	25 puntos Zona de riesgo muy alto Evitar- gestionar el riesgo Requiere acción inmediata
A	4	4 puntos Zona de riesgo muy bajo Asumir el riesgo	8 puntos Zona de riesgo bajo Administrar el riesgo	12 puntos Zona de riesgo moderado Reducir el riesgo a niveles más bajos	16 puntos Zona de riesgo alto Evitar la gestión de los riesgos	20 puntos Zona de riesgo muy alto Evitar- gestionar el riesgo Requiere acción inmediata
M	3	3 puntos Zona de riesgo muy bajo Asumir el riesgo	6 puntos Zona de riesgo bajo Administrar el riesgo	9 puntos Zona de riesgo bajo Administrar el riesgo	12 puntos Zona de riesgo moderado Reducir el riesgo a niveles más bajos	15 puntos Zona de riesgo alto Evitar la gestión de los riesgos
B	2	2 puntos Zona de riesgo muy bajo Asumir el riesgo	4 puntos Zona de riesgo muy bajo Asumir el riesgo	6 puntos Zona de riesgo bajo Administrar el riesgo	8 puntos Zona de riesgo bajo Administrar el riesgo	10 puntos Zona de riesgo moderado Reducir el riesgo a niveles más bajos
MB	1	1 puntos Zona de riesgo muy bajo Asumir el riesgo	2 puntos Zona de riesgo muy bajo Asumir el riesgo	3 puntos Zona de riesgo muy bajo Asumir el riesgo	4 puntos Zona de riesgo muy bajo Asumir el riesgo	5 puntos Zona de riesgo bajo Administrar el riesgo

Fuente: [35]

Una vez definido las zonas de riesgo a las cuales está expuesto cada activo que posee la empresa se procedió a la evaluación de estos y a su clasificación basándonos en la clasificación que se indica en la Tabla 25. A continuación en la Tabla 26 se muestra un ejemplo de cómo se realizó esta clasificación de los riesgos. Para poder observar la valoración de todos los activos que posee la empresa se debe revisar el Anexo 11.

Tabla 26. Análisis de riesgos mediante la matriz de calor

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B

Fuente: Autores del Proyecto

Con los datos obtenidos en la matriz de calor se generó los siguientes gráficos en los cual se pueden observar la distribución del riesgo en los activos que posee la empresa.

En la mayoría de los activos físicos que posee la empresa se puede observar que existe un riesgo bajo y medio lo cual nos indica que estos riesgos no son tan peligrosos para estos activos.

Tabla 27. Riesgos en los activos físicos

Hardware	Riesgo
MA	0
A	1
M	14
B	39
MB	9

Fuente: Autores del proyecto

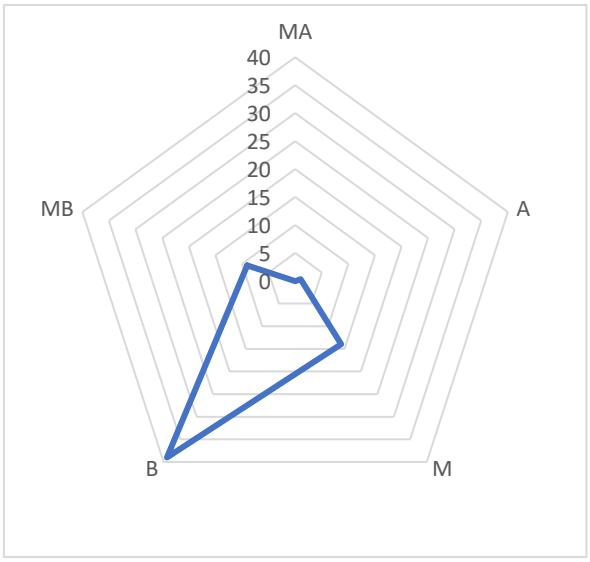


Figura 14. Distribución del riesgo en los activos hardware

Fuente: Anexo 11

En lo referente a los activos de software se pudo observar que la distribución del riesgo se centra en los niveles bajo y alto lo cual nos indica que estos activos están expuestos a riesgos considerables. Aunque también se debe tener en cuenta los valores de los riesgos muy altos y medios ya que poseen una valoración media.

Tabla 28. Riesgos en los activos de software

Software	**Riesgo**
MA	6
A	12
M	6
B	14
MB	2

Fuente: Autores del Proyecto

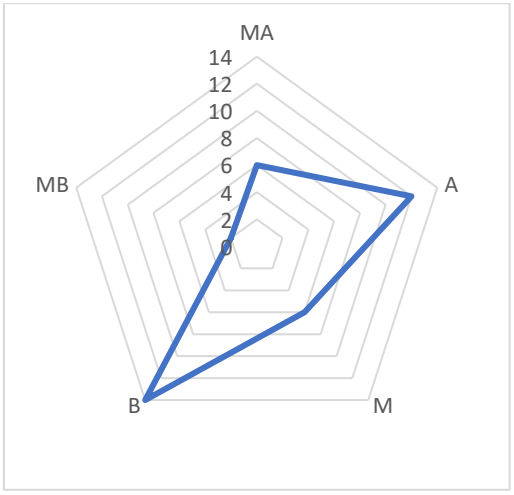


Figura 15. Distribución del riesgo en los activos de software

Fuente: Anexo 11

En los activos de personal se puede observar que existe riesgos de nivel muy alto y alto por lo cual se debería ejecutar medidas que ayuden a disminuir estos riesgos lo antes posible.

Tabla 29. Riesgos en los activos personal

Personal	Riesgo
MA	5
A	4
M	3
B	0
MB	5

Fuente: Autores del Proyecto

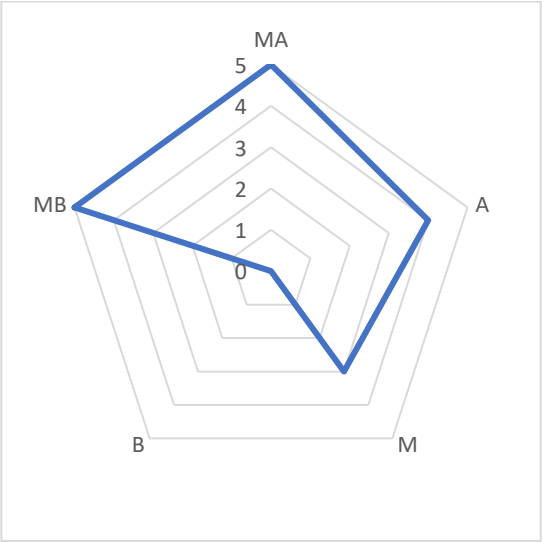


Figura 16. Distribución del riesgo en los activos personales

Fuente: Anexo 11

Por su parte los activos de información están expuestos en su mayoría a riesgos altos, moderados y bajo lo cual nos indica que igual que con los activos de personal se debe realizar acciones de mitigación lo más pronto posible para de esta forma proteger estos activos de forma correcta.

Tabla 30.Riesgos de los activos de información

Información	Riesgo
MA	5
A	15
M	12

B	6
MB	0

Fuente: Autores del Proyecto

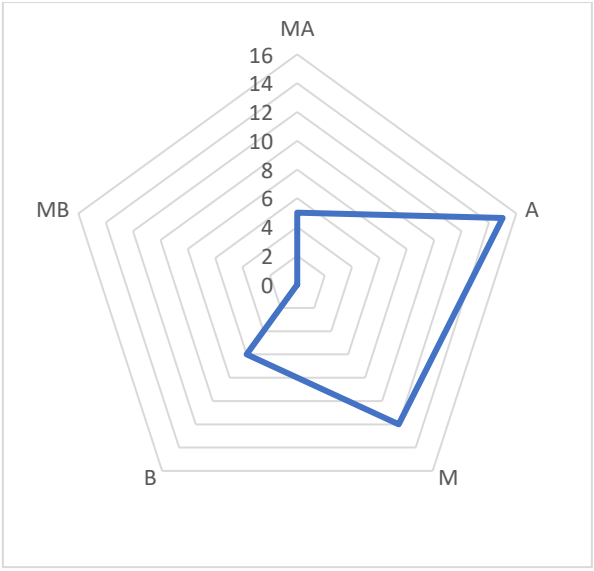


Figura 17. Distribución del riesgo en los activos de información

Fuente: Anexo 11

En lo referente a los riesgos a los cuales pueden estar expuestos las instalaciones se posee un nivel bajo lo cual nos indica que los riesgos a los cuales están sometidas las instalaciones de la empresa se los puede prevenir o mitigar de forma rápida.

Tabla 31.Riesgos de las instalaciones

Instalaciones	**Riesgo**
MA	1
A	0
M	3
B	11
MB	0

Fuente: Autores del Proyecto

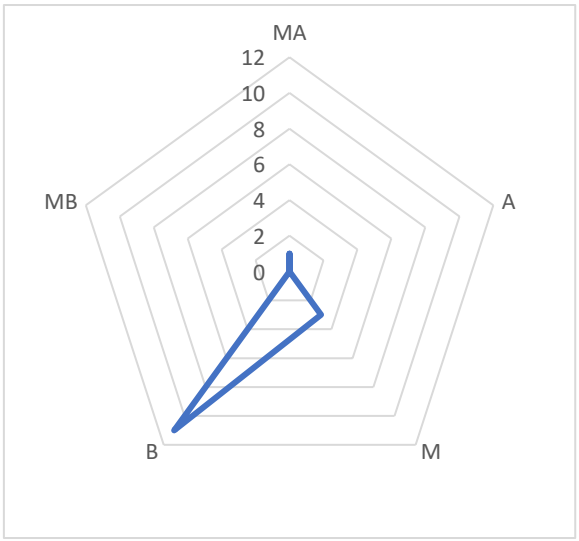


Figura 18. Distribución del riesgo en las instalaciones

Fuente: Anexo 11

En lo referente a los servicios que brinda la empresa se pudo evidenciar que existe un nivel de riesgo muy bajo y alto por lo cual la empresa debería tomar en cuenta acciones correctivas que disminuyan estos riesgos para garantizar un buen servicio a los clientes.

Tabla 32. Riesgos de los servicios

Servicios	**Riesgo**
MA	0
A	2
M	0
B	1
MB	2

Fuente: Autores del Proyecto

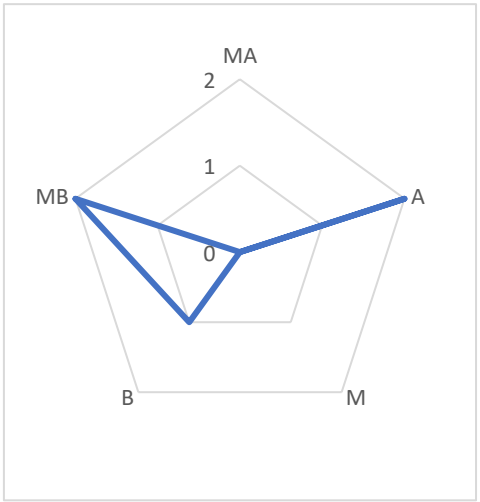


Figura 19. Distribución del riesgo en los activos de servicios

Fuente: Anexo 11

Finalmente, los riesgos relacionados a los equipos auxiliares son muy bajos los cual nos indica que la empresa posee un correcto control de estos equipos.

Tabla 33.Riesgos de los equipos auxiliares

E. Auxiliares	Riesgo
MA	0
A	1
M	1
B	6
MB	12

Fuente: Autores del Proyecto

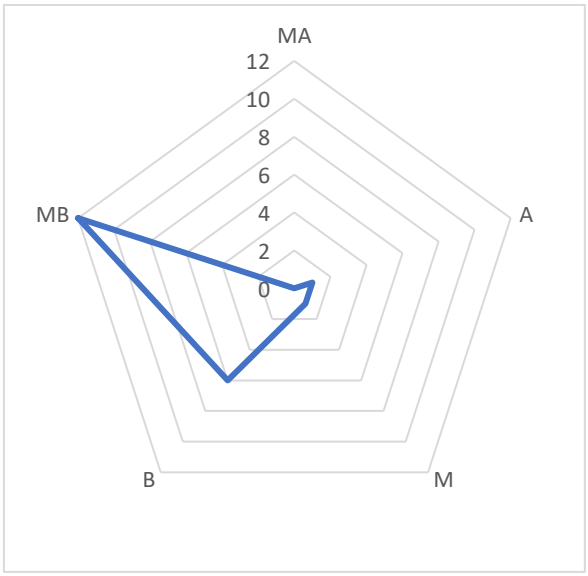


Figura 20. Distribución del riesgo en los activos de equipamiento auxiliar

Fuente: Anexo 11

4.6.5. Salvaguardas

Las salvaguardas son los procedimientos, contra medidas o mecanismos tecnológicos los cuales ayudan a reducir el riesgo, ya que en la práctica no es frecuente encontrar sistemas desprotegidos. Para nuestro caso de estudio las salvaguardas que posee la empresa Ultralink se las muestra en la Tabla 34. Para poder observar todas las salvaguardas que posee la empresa mirar el Anexo 12 ya que la tabla que se presenta a continuación es solo un ejemplo de estas.

Tabla 34. Identificación de los controles existentes

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo	Controles existentes
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo

Fuente: Autores del Proyecto

4.7. Tratamiento del riesgo

Una vez se han evaluado los riesgos se procede a su tratamiento para lo cual se debe tener en cuenta los criterios de aceptación del riesgo. Según la ISO 27001: 2013 existen cuatro opciones que nos ayudan a dar un correcto tratamiento a los riesgos, estas opciones no son unos criterios absolutos ni son excluyentes entre sí por lo cual se los puede combinar y de esta forma abordar a más de un riesgo, las opciones antes mencionadas son las siguientes [36]:

4.7.1. Aceptación del riesgo

Es el nivel de riesgo aceptable en el cual no es necesario implementar nuevos controles ya que el riesgo existente se lo puede manejar, sin embargo, se debe tener un constante monitoreo y revisión periódica de los mismos con el fin de responder oportunamente ante su materialización.

4.7.2. Reducción del riesgo

Cuando el nivel de riesgo es superior al criterio de aceptación se debe realizar una correcta selección de controles los cuales ayuden a disminuir el riesgo hasta un nivel adecuado. Entre los controles que se puede implementar para la reducción del riesgo tenemos [36]:

- Controles de prevención
- Controles de corrección
- Controles para la detección
- Controles para la minimización del impacto
- Controles de disuasión
- Controles de monitoreo y concientización
- Controles de recuperación

Cabe recalcar que no siempre se puede implementar los controles antes mencionados ya que existen algunas restricciones las cuales pueden afectar su uso.

4.7.3. Transferencia del riesgo

Esta opción se la puede emplear cuando el riesgo se lo puede compartir o transferir a una entidad externa la cual pueda manejar este riesgo de una forma más eficiente. Al utilizar este tipo de tratamiento se debe tener muy claro que se puede trasferir la responsabilidad del tratamiento del riesgo, pero la responsabilidad sobre el impacto no, ya que los clientes que fueron afectados por algún evento adverso siempre atribuirán las fallas a la organización.

4.7.4. Evitación del riesgo

Cuando los riesgos son muy altos solucionar este tipo de riesgos tiene un costo que sobrepasa los beneficios que se obtendrían de solucionarlo, por lo tanto, se procede a evitar por completo este tipo de riesgos, por lo cual se procede a eliminar o modificar las actividades o procedimientos que pueden ser la causa de dichos riesgos [36].

4.7.5. Criterios para el tratamiento del riesgo

Con las cuatro opciones antes mencionadas se procede a establecer el tratamiento correspondiente a cada una de las zonas que se pudo determinar mediante el cálculo del riesgo. A continuación, en la Tabla 35 se muestra un ejemplo de cómo se establece los tratamientos adecuados para cada uno de los riesgos. Para poder observar todos los datos de esta clasificación se debe acceder al Anexo 13.

Tabla 35. Opciones de tratamientos de riesgos

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo	Controles existentes	Opciones de tratamiento del riesgo
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B	No aplica	Aceptar riesgo
	No existe control sobre las personas que	Robo	2	2	4	MB	No aplica	Aceptar riesgo

	ingresan y salen de la organización							

Fuente: Autores del Proyecto

4.7.6. Acciones correctivas para el tratamiento del riesgo

Como los riesgos a los cuales están expuestos los activos que posee la empresa son de diferente nivel las acciones propuestas en el presente trabajo están centradas en los riesgos de nivel medio, alto y muy alto. A continuación, se muestra una tabla de un ejemplo de las acciones que se aplicaran a los riesgos antes mencionados. Para poder ver todas las acciones que se implementaran en los riesgos mirar el Anexo 14.

Tabla 36. Acciones correctivas para el tratamiento del riesgo

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del riesgo	Magnitud del riesgo	Controles existentes	Opciones de tratamiento del riesgo	Acciones de tratamiento	Justificación
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	12	M	Extintores, Alarmas de humo	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incendios
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	12	M	No aplica	Reducir riesgo	Restricción de acceso, Incorporar videovigilancia	Las acciones antes mencionadas generan un mejor control en las instalaciones de la empresa

	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al ingresar a las redes de la empresa	No se posee seguridad en la gestión de las redes
S.O Windows	Errores en la configuración de seguridad	Ciberataques	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Transferir el riesgo	Capacitar al personal, Escaneo de dispositivos Generar redes de invitados para personal externo	En la actualizad en la empresa no se realiza ninguna de las acciones antes mencionadas por lo cual no existe este tipo de control
	Ausencia de documentación de uso	Modificación sin autorización	16	A	No aplica	Reducir o Transferir el riesgo	Generar documentos de usuario	No existe la documentación
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	Capacitación online	Reducir riesgo	Generar documentos de usuario	No existe la documentación
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	16	A	Capacitación online	Reducir o Transferir el riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de contraseñas y su manipulación	No existe capacitación al personal

Fuente: Autores del Proyecto

4.8. Riesgo residual

Es el riesgo existente posterior a la evaluación del riesgo mediante los criterios de tratamiento. Para obtener este riesgo se lo realiza mediante la multiplicación del impacto residual por el posible impacto, la obtención de estos valores se lo realiza luego de la degradación del riesgo inicial teniendo en cuenta la eficiencia de los tratamientos seleccionados [33].

Una vez se ha realizado la implementación de las acciones mencionados en la tabla anterior se procedió a realizar el cálculo del riesgo residual. En la Tabla 37, a continuación, se muestra un ejemplo como se realizó este cálculo, para poder observar todos los datos de esta valoración revisar el Anexo 15.

Tabla 37. Cálculo del riesgo residual

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad residual			Valor del riesgo residual	Magnitud del riesgo
				Degradación	Probabilidad	Total		
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	2	2	2	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	1	1	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	2	2	2	4	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	2	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB

Fuente: Autores del Proyecto

4.9. Objetivos de control y controles

Posterior a obtener los resultados de la evaluación de los riesgos y haber verificado el nivel de impacto y riesgos a los cuales están expuestos los activos y luego de analizar las opciones de tratamiento adecuados para lograr la mitigación de los riesgos. La mayoría de las amenazas que se han podido

evidenciar pueden ser tratadas mediante la reducción de los niveles de riesgo por lo cual se seleccionarán los objetivos de control y controles que se encuentran en la norma ISO/IEC 27001: 2013 ya que gracias a estos controles se podrán diseñar las políticas para la empresa. También se debe tener en cuenta que para obtener una correcta solución de las amenazas se debe implementar más de un control.

En la Tabla 38 se muestran cuáles son los objetivos de control y los controles que se encuentran en la norma ISO/IEC 27001: 2013.

Tabla 38. Objetivos de control y controles de la ISO 27001: 2013

Dominio	Objetivos de control	Controles
A.5. Políticas de Seguridad de la Información	A.5.1. Directrices de la Dirección en Seguridad de la Información	A.5.1.1. Conjunto de políticas para la seguridad de la información
		A.5.1.2. Revisión de las políticas para la seguridad de la información
A.6. Aspectos Organización de la Seguridad de la Información	A.6.1. Organización Interna	A.6.1.1. Funciones y responsabilidades de la seguridad de la información
		A.6.1.2. Segregación de tareas
		A.6.1.3. Contacto con las autoridades
		A.6.1.4. Contacto con grupos de interés especial
		A.6.1.5. Seguridad de la información en la gestión de proyectos
	A.6.2. Dispositivos Móviles y Teletrabajo	A.6.2.1. Política de uso de dispositivos móviles
		A.6.2.2. Teletrabajo
A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.1. Investigación de antecedentes
		A.7.1.2. Términos y condiciones de contratación
	A.7.2. Durante la contratación	A.7.2.1. Responsabilidades de gestión
		A.7.2.2. Concienciación, educación y capacitación en seguridad de la información
		A.7.2.3. Proceso disciplinario
	A.7.3. Cese o cambio de puesto de trabajo	A.7.3.1. Cese o cambio de puesto de trabajo
A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.1. Inventario de activos
		A.8.1.2. Propiedad de los activos
		A.8.1.3. Uso aceptable de los activos

		A.8.1.4. Devolución de activos
	A.8.2. Clasificación de la información	A.8.2.1. Directrices de clasificación
		A.8.2.2. Etiquetado y manipulado de la información
		A.8.2.3. Manipulación de activos
	A.8.3. Manejo de los soportes de almacenamiento	A.8.3.1. Gestión de medios removibles
		A.8.3.2. Eliminación de soportes
		A.8.3.3. Soportes físicos en tránsito
A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.1. Política de control de acceso
		A.9.1.2. Control de acceso a las redes y servicios asociados
	A.9.2. Gestión de acceso de usuarios	A.9.2.1. Gestión de altas/bajas en el registro de usuarios
		A.9.2.2. Gestión de los derechos de acceso asignados a usuarios
		A.9.2.3. Gestión de derechos de acceso con privilegios especiales
		A.9.2.4. Gestión de información confidencial de autenticación de usuarios
		A.9.2.5. Revisión de los derechos de acceso de usuarios
		A.9.2.6. Cancelación o ajuste de los derechos de acceso
	A.9.3. Responsabilidades de los usuarios	A.9.3.1. Uso de información confidencial para la autenticación
	A.9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1. Restricción de acceso a la información
		A.9.4.2. Procedimientos seguros de inicio de sesión
		A.9.4.3. Gestión de contraseñas de usuario
		A.9.4.4. Uso de herramientas de administración de sistemas
		A.9.4.5. Control de acceso al código fuente de programas
A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.1. Política sobre el uso de controles criptográficos
		A.10.1.2. Gestión de Claves.
A.11. Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.1. Perímetro de seguridad física
		A.11.1.2. Controles físicos de entrada
		A.11.1.3. Seguridad de oficinas, despachos y recursos
		A.11.1.4. Protección contra amenazas externas y ambientales
		A.11.1.5. Trabajo en áreas seguras.

		A.11.1.6. Áreas de acceso público, despacho y carga.
	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos
		A.11.2.2. Instalaciones de suministro
		A.11.2.3. Seguridad del cableado
		A.11.2.4. Mantenimiento de los equipos
		A.11.2.5. Retiro de bienes
		A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones
		A.11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento
		A.11.2.8. Equipos desatendidos por los usuarios
		A.11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla
A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación
		A.12.1.2. Gestión de cambios
		A.12.1.3. Gestión de Capacidad
		A.12.1.4. Separación de los ambientes de desarrollo, prueba y producción
	A.12.2. Protección contra códigos maliciosos	A.12.2.1. Controles contra códigos maliciosos
	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información
	A.12.4. Registro de actividad y supervisión	A.12.4.1. Registro de eventos.
		A.12.4.2. Protección de los registros de información
		A.12.4.3. Registros de actividad del administrador y operador del sistema
		A.12.4.4. Sincronización de relojes
	A.12.5. Control de software en la producción	A.12.5.1. Instalación de software en sistemas operativos
	A.12.6. Gestión de vulnerabilidad técnica	A.12.6.1. Gestión de las vulnerabilidades técnicas
		A.12.6.2. Restricciones sobre la instalación de software
	A.12.7. Consideraciones de las auditorías de los sistemas de información	A.12.7.1. Controles de auditorías de los sistemas de información
A.13. Seguridad de las Comunicaciones	A.13.1. Gestión de Seguridad en las redes	A.13.1.1. Controles de redes
		A.13.1.2. Seguridad de los servicios de red

		A.13.1.3. Separación en las redes
	A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información
		A.13.2.2. Acuerdos de intercambio de información
		A.13.2.3. Mensajería electrónica
		A.13.2.4. Acuerdos de confidencialidad y de no divulgación
A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.1. Requisitos de seguridad de los sistemas de información	A.14.1.1. Análisis y especificación de los requisitos de seguridad de la información
		A.14.1.2. Aseguramiento de los servicios de aplicaciones en las redes públicas
		A.14.1.3. Protección de las transacciones en línea
	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.1. Política de desarrollo seguro de software
		A.14.2.2. Procedimiento de control de cambios en los sistemas
		A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo
		A.14.2.4. Restricciones sobre los cambios de paquetes de software
		A.14.2.5. Uso de principios de ingeniería en protección de sistemas
		A.14.2.6. Ambiente de desarrollo seguro
		A.14.2.7. Externalización del desarrollo de software
		A.14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas
		A.14.2.9. Pruebas de aceptación de sistemas
	A.14.3. Datos de prueba	A.14.3.1. Protección de los datos utilizados en pruebas
A.15. Relaciones con los Proveedores	A.15.1. Seguridad de la información en las relaciones con los proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores
		A.15.1.2. Tratamiento del riesgo dentro de los acuerdos con los proveedores
		A.15.1.3. Cadena de suministro en tecnologías de información y comunicación
	A.15.2. Gestión de la prestación de servicios de proveedores	A.15.2.1. Supervisión y revisión de los servicios prestados por terceros
		A.15.2.2. Gestión de cambios en los servicios de los proveedores
A.16. Gestión de Incidentes de Seguridad de la Información	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1. Responsabilidades y procedimientos
		A.16.1.2. Notificación de los eventos de seguridad de la información
		A.16.1.3. Notificación de puntos débiles de la seguridad

		A.16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones
		A.16.1.5. Respuesta a incidentes de seguridad de seguridad
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información
		A.16.1.7. Recolección de evidencia
A.17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	A.17.1. Continuidad de la seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información
		A.17.1.2. Implementación de la continuidad de la seguridad de la información
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información
A.18. Cumplimiento	A.18.1. Cumplimiento de los requisitos legales y contractuales	A.18.1.1. Identificación de la legislación aplicable
		A.18.1.2. Derechos de Propiedad Intelectual
		A.18.1.3. Protección de los registros de la organización
		A.18.1.4. Protección de datos y privacidad de la información personal
		A.18.1.5. Regulación de los controles criptográficos
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información
		A.18.2.2. Cumplimiento de las políticas y normas de seguridad
		A.18.2.3. Revisión del cumplimiento técnico

Fuente: [37] [38] [39]

4.9.1. Declaración de aplicabilidad de los controles

Luego de haber analizado los riesgos a los cuales pueden estar expuestos los activos se procedió a evaluar los controles que se posee en la ISO 27001 y posterior a ello se procedió a realizar la declaración de aplicabilidad de los mismos teniendo en cuenta la justificación de su utilización o no. A continuación, se muestra un ejemplo de cómo se realizó esta justificación de aplicabilidad, para poder observar todos los datos revisar el Anexo 16.

Tabla 39. Declaración de aplicabilidad de los controles

Dominio	Objetivos de control	Controles	Aplicabilidad	Justificación
A.5. Políticas de Seguridad	A.5.1. Directrices de la Dirección en	A.5.1.1. Conjunto de políticas para la	Si	Se debe crear un conjunto de políticas

de la Información	Seguridad de la Información	seguridad de la información		para la seguridad de la información las cuales sean aprobadas por la Dirección y posterior a ello deben ser publicadas y comunicadas a los empleados y partes interesadas de la empresa.
		A.5.1.2. Revisión de las políticas para la seguridad de la información	Si	Las políticas de seguridad de la Información deben ser revisadas en intervalos de tiempo para asegurar la eficacia de las mismas.

Fuente: Autores del Proyecto

4.9.2. Selección de objetivos de control y controles

Luego de analizar los datos obtenidos sobre los niveles de riesgos a los cuales están expuestos los activos que posee la empresa se procedió a seleccionar los objetivos de control y los controles óptimos para poder dar un tratamiento optimo a los riesgos. En la Tabla 40 se muestra un ejemplo de cómo se realizó esta selección la cual nos servirá como base para la creación de las políticas de seguridad. Para poder observar todos los datos revisar el Anexo 17.

Tabla 40. Selección de objetivos de control y controles

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del riesgo residual	Magnitud del riesgo	Dominio	Objetivos de control	Controles	Justificación de aplicabilidad
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio	Sobrecalentamiento y daño de los	6	B	A.11.Seguridad Física y	A.11.2. Seguridad de	A.11.2.2. Instalacio	Se establecen medidas de control para el

	sistema de refrigeración	equipos en el data center			Ambiental	los equipos	nes de suministro	suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad

Fuente: Autores del Proyecto

4.10. Roles y Responsabilidades en el SGSI

Debido a que la empresa Ultralink no posee un área de seguridad de la información no se puede generar una correcta distribución de las responsabilidades, pero teniendo en cuenta los perfiles de los responsables que debe posee un área de seguridad se sugiere que la empresa incluya los siguientes cargos para poder implementar el SGSI:

- **Comité de gestión:** Es el comité que se encarga de gestionar y controlar la implementación del SGSI, este comité tendrá la capacidad de tomar las decisiones de seguridad por lo cual debe estar constituido por personal de diferentes áreas las cuales estén involucradas directa o indirectamente en los procesos del sistema de gestión de seguridad de la información.
- **Comité de dirección:** Es el comité encargado de tomar las decisiones de seguridad que afecten a los temas administrativos, legales, recursos humanos y tecnología por lo cual se sugiere que el comité debe estar conformado por los directores de estas áreas ya que mínimo debe existir un representante de cada una de las áreas antes mencionadas.
- **Responsable de seguridad:** El responsable de la seguridad será el que tendrá línea directa con la gerencia ya que hay decisiones que se deben implementar de forma inmediata. Este responsable debe poseer el respaldo de las máximas autoridades lo cual generara en la voz de mando dentro de la empresa, las funciones que desempeñara esta

persona serán las de mantener la confidencialidad, integridad y disponibilidad de los activos de información que posee la empresa.

4.11. Definición de Políticas, estándares y procedimientos

Una vez que hemos realizado la evaluación de los riesgos y se ha seleccionado los controles para el tratamiento de los riesgos es necesario establecer políticas de seguridad las cuales nos permitan gestionar de manera adecuada los procesos y normas de seguridad. Las políticas deben incluir la definición de las responsabilidades y estar documentadas. Para la generación de las políticas se debe tomar en cuenta el modelo propuesto por la norma ISO/IEC 27002 el cual nos permite establecer los lineamientos y principios generales.

4.11.1. Diseño de las políticas

Para el diseño de las políticas se lo hará según las necesidades de seguridad que poseen los activos y en base a la norma ISO/IEC 27002. En estas políticas se incluyen los lineamientos y normas que deben ser cumplidos por los colaboradores y personal externo que tenga acceso a los activos que posee la empresa, para poder minimizar el riesgo a los cuales tan expuestos los activos se debe dar cumplimiento a las políticas para lo cual debe existir una correcta divulgación de las mismas.

A continuación, se muestra un ejemplo de una política de seguridad que se podría implementar en Ultralink, para poder observar todas las políticas propuestas se debe revisar el Anexo 18.

Tabla 41.Política de seguridad para controlar el acceso físico y del entorno

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE CONTROL DE ACCESO FÍSICA Y DEL ENTORNO		
OBJETIVO:	Controlar el acceso físico no autorizado, prevenir los daños o robos de los activos de la empresa mediante la utilización de mecanismos de acceso físico o lógico.	

ALCANCE:	La presente política es aplicable a todo el personal, visitantes y proveedores que requieran ingresar a las instalaciones de la empresa
REFERENCIA:	11.1. Áreas seguras 11.1.1. Perímetro de seguridad física 11.1.2. Controles físicos de entrada 11.1.4. Protección contra amenazas externas y ambientales

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Cuando no exista supervisión verificar que las entradas a las instalaciones estén cerradas de forma correcta.
- Toda persona que no pertenezca a la empresa y desee ingresar a las instalaciones de Ultralink debe registrarse y solicitar la autorización de ingreso.
- Implementar mecanismos de examinación de bolsos, maletas, cajas, etc. que se deseen ingresar a las instalaciones.
- Implementar un monitoreo permanente de los ingresos lo cual ayudara a identificar accesos no autorizados.
- Todo el personal de la empresa debe portar su identificación en un lugar visible mientras permanezca dentro de las instalaciones.
- Se debe eliminar lo más pronto posible los permisos de acceso físico al personal que termine su vinculación con la empresa
- Se debe realizar la devolución del identificador institucional tan pronto se termine la vinculación del personal.
- Implementar planes de emergencia o de contingencia ante alguna amenaza externa.
- Mantener en estado optimo la infraestructura física que posee la empresa, es decir las paredes deben ser sólidas y resistentes.
- Separar las áreas que puedan contener activos importantes para la empresa.
- Impartir capacitaciones las cuales ayuden a disminuir los riesgos naturales.

RESPONSABILIDADES:

- Todos los coordinadores o supervisores deben asegurarse de que el personal que se encuentre bajo su cargo este informado de forma correcta y le dé cumplimiento a esta política.
- Por parte de la gerencia debe proporcionar todas las herramientas que sean necesarias para tener un acceso correcto.

Fuente: [40] [41]

4.12. Socialización y Capacitación del SGSI

Para que las políticas de seguridad que se han creado en el punto anterior sean eficientes, todo el personal que constituye la empresa Ultralink y si es necesario los proveedores deben ser capacitados sobre la importancia de la seguridad de la información y los procedimientos que se deben emplear pada dar un correcto uso de esta información. Para la ejecución de estas capacitaciones deben existir responsables los cuales ayuden a socializar estos temas, entre los responsables tenemos:

- **Personal de seguridad:** Sera el personal experto en seguridad el cual se encargará de capacitar al ´personal sobre la seguridad y las buenas prácticas.
- **Personal de sistemas:** Serán los encargados de comprender y dar cumplimiento a los controles de seguridad que se implementen en los sistemas que se encuentren a su cargo.
- **Usuarios finales:** Serán los que reciban la capacitación y deberán poner total interés en la capacitación para obtener los nuevos conocimientos.

La capacitación debe ser distribuida en varias sesiones lo cual no interrumpa el funcionamiento de la empresa y también de esta forma el personal puede comprender de mejor manera los conceptos impartidos, el tiempo que se podría destinar para cada una de estas sesiones podría ser de una hora. El material que se emplearía para las capacitaciones debe ser interactivo y contener información relevante del tema a ser tratado. Como un método de repaso el personal recibirá en su correo la materia que se empleó en la capacitación, una vez finalizada la capacitación la institución debe generar actividades de evaluación las cuales ayuden a verificar el grado de aprendizaje que se ha obtenido en las capacitaciones. En caso de que las evaluaciones que se han tomado al personal no cumplan con una nota satisfactoria se debe implementar retroalimentaciones periódicas con el fin de crear la persona con conciencia sobre la seguridad de la información y su correcto uso.

4.13. Plan de implementación

Para la implementación de este Sistema de Gestión de Seguridad de la Información se debe seguir las siguientes fases:

- **Fase de aprobación:** En esta fase se debe obtener la aprobación de la alta gerencia para iniciar la implementación del SGSI, una vez se haya obtenido el visto bueno se debe generar los límites que tendrá la implementación de este modelo y sus requerimientos.
- **Fase de planificación:** En esta fase se tomará en cuenta el alcance que tendrá en SGSI, se distribuirán las responsabilidades y evaluarán los resultados que se obtuvieron de la evaluación de los riesgos a los cuales están expuestos los activos de Ultralink.
- **Fase de implementación:** En esta fase se pondrán en ejecución los controles los cuales deben ser monitoreados de forma permanente para obtener mejores resultados de su implementación.
- **Fase de optimización:** En esta fase se deberá elaborar un plan de priorización para de esta forma dar una solución de forma eficiente a los riesgos.

4.14. Recepción y análisis del diseño del SGSI por parte de Ultralink

La empresa Ultralink ha recibido toda la documentación que se generó al momento de diseñar el SGSI. Posterior al análisis que realizó la empresa sobre la información que se le otorgo y la verificación sobre esta sobre los cumplimientos de los lineamientos que se plantearon al inicio de este trabajo finalmente la institución confirió un certificado de aprobación en el cual se detalla que la empresa está conforme con el presente trabajo. El certificado antes mencionado se encuentra en el Anexo 19.

4.15. Discusión y resultados

Los resultados que se obtuvieron en el presente proyecto fueron generados para dar cumplimiento a los objetivos que se establecieron anteriormente por lo cual se generaron las siguientes actividades:

- Reuniones periódicas para recopilación de información.

- Desarrolló un diagnóstico inicial sobre los niveles de seguridad que poseía la empresa y la madurez de los mismos.
- Generación de inventario de activos.
- Identificación de amenazas y vulnerabilidades que pueden afectar los activos de la empresa.
- Valoración de los riesgos.
- Identificación de aplicabilidad de los controles en la empresa.
- Desarrollo de políticas de seguridad.
- Entrega de resultado a las partes interesadas de la empresa.

Para el desarrollo de las actividades antes mencionadas se procedió a la utilización de entrevistas, manuales, guías, documentación física y digital, etc. A continuación, se explican algunos puntos de vista que se obtuvieron de los resultados.

Para el desarrollo de este proyecto se procedió a realizar una comparación entre las metodologías de gestión de riesgo, gracias a esto se seleccionó la metodología MAGERIT la cual es muy útil al momento de iniciar el proceso de gestión de la seguridad de la información ya que esta metodología se enfoca en la minimización de los riesgos críticos para el funcionamiento óptimo de la empresa.

Luego de una auditoria inicial basada en los controles que posee la ISO 27001 se pudo evidenciar que la empresa Ultralink no cumple con la mayoría de estos controles, por lo cual tiene múltiples falencias en la seguridad de la información las cuales en su mayoría deben ser atendidas lo más pronto posible.

El nivel de cumplimiento que posee la empresa sobre los requerimientos de seguridad que se plantea en el Anexo A de la norma ISO/IEC 27001 es muy bajo ya que la mayoría de los controles se encuentran en un porcentaje menor al 33% lo cual implica que la empresa no posee controles de seguridad o muchos de estos controles son desconocidos para la empresa.

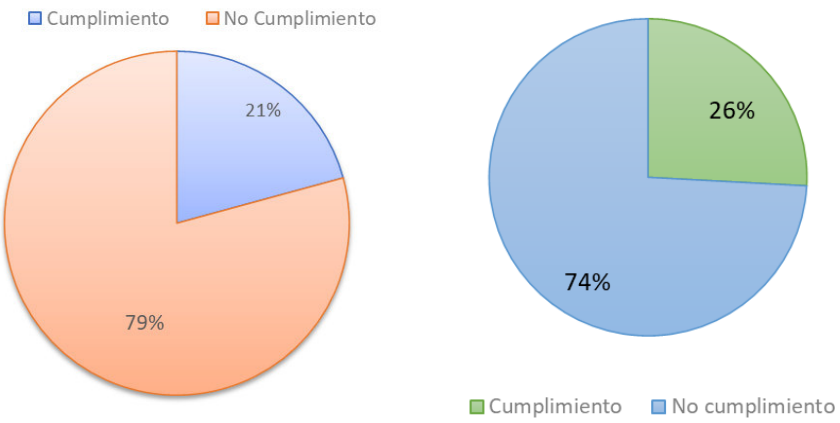


Figura 21.Niveles de cumplimiento del Anexo A

Fuente: Autores del Proyecto

Gráficamente la distribución de los controles que plantea el Anexo A de la ISO 27001 que posee la empresa son los siguientes

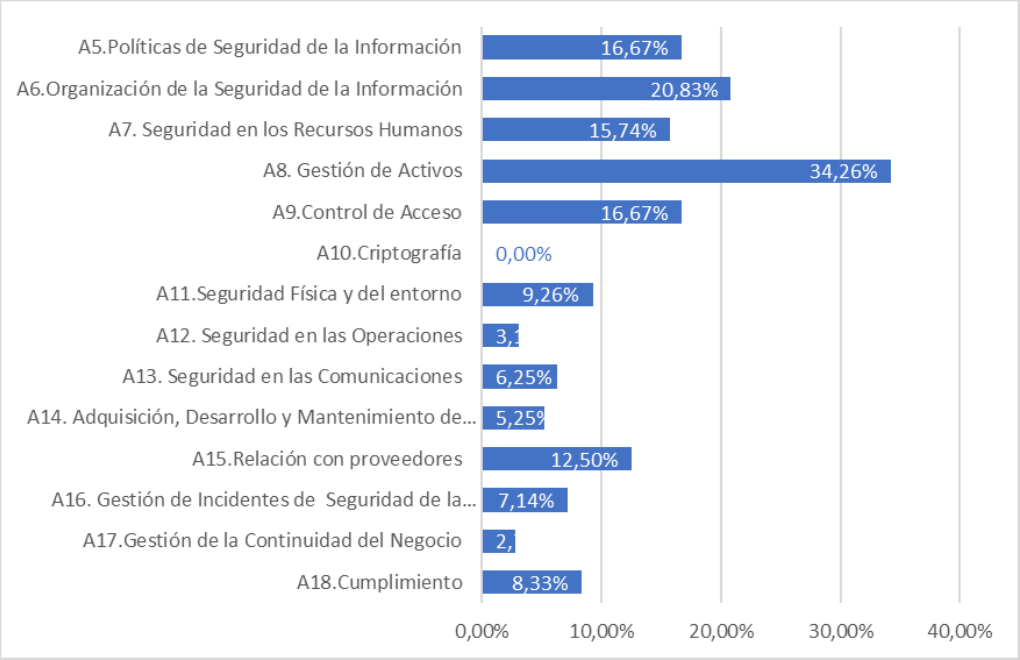


Figura 22.Cumplimiento inicial de los controles de la ISO 27001

Fuente: Autores del Proyecto

Luego de analizar y valorar los activos informáticos que posee la empresa se pudo determinar la criticidad a la cual están expuestos los activos además de poder identificar la importancia que estos poseen para la empresa, por lo cual se requiere implementar un plan de capacitación en seguridad de la información el cual ayude a fortalecer en los empleados una cultura de seguridad y de esta manera mejorar la seguridad de la información de la empresa.

Otro de los factores que se debe tomar en cuenta es que al no poseer controles que ayuden a proteger el intercambio de información con terceros, la entidad puede ser afectada de forma negativa causando un deterioro en su imagen ante los clientes a los cuales brinda sus servicios por lo cual es indispensable implementar de forma inmediata mecanismos de cifrado los cuales ayuden a garantizar la confidencialidad e integridad de la información.

Con el diseño del SGSI y su posterior implementación no se garantiza un total aseguramiento de los activos informáticos que posee la empresa ya que esta implementación no permite gestionar de forma correcta los riesgos de gran impacto porque estos deben ser resueltos por profesionales especializados en seguridad de la información.

Todas las políticas, procedimientos y controles de seguridad que se quieran implementar en Ultralink deben tener el apoyo de la dirección ya que ellos serán los que velen por el correcto funcionamiento de estas, también se debe tener en cuenta que las políticas deben ser implementadas según los requerimientos de seguridad de cada área, su alcance y las responsabilidades por lo cual esta tarea debe ser coordinada entre todos los responsables de cada área y posteriormente informaran a el personal que se encuentra bajo su responsabilidad.

Se espera que luego del despliegue de este proyecto los niveles de cumplimiento de los controles que se encuentran en el Anexo A de la ISO 27001 sean los siguientes:

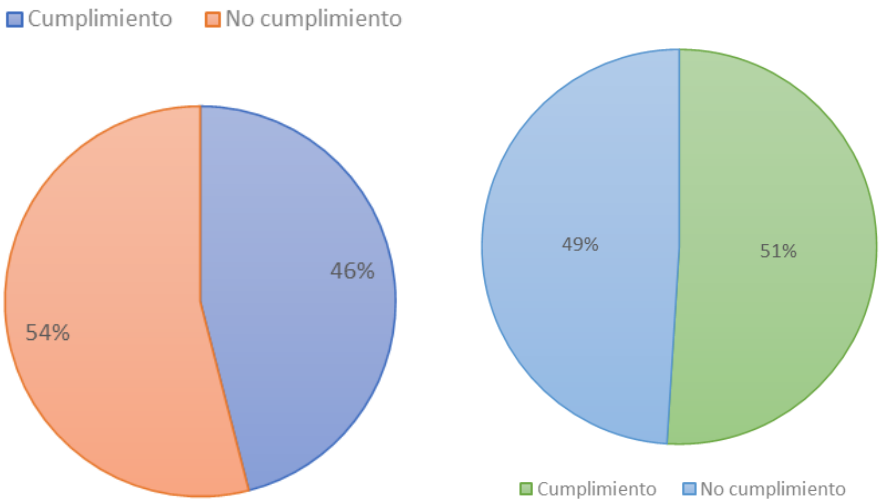


Figura 23.Cumplimiento del Anexo A posterior a la implementación

Fuente: Autores del Proyecto

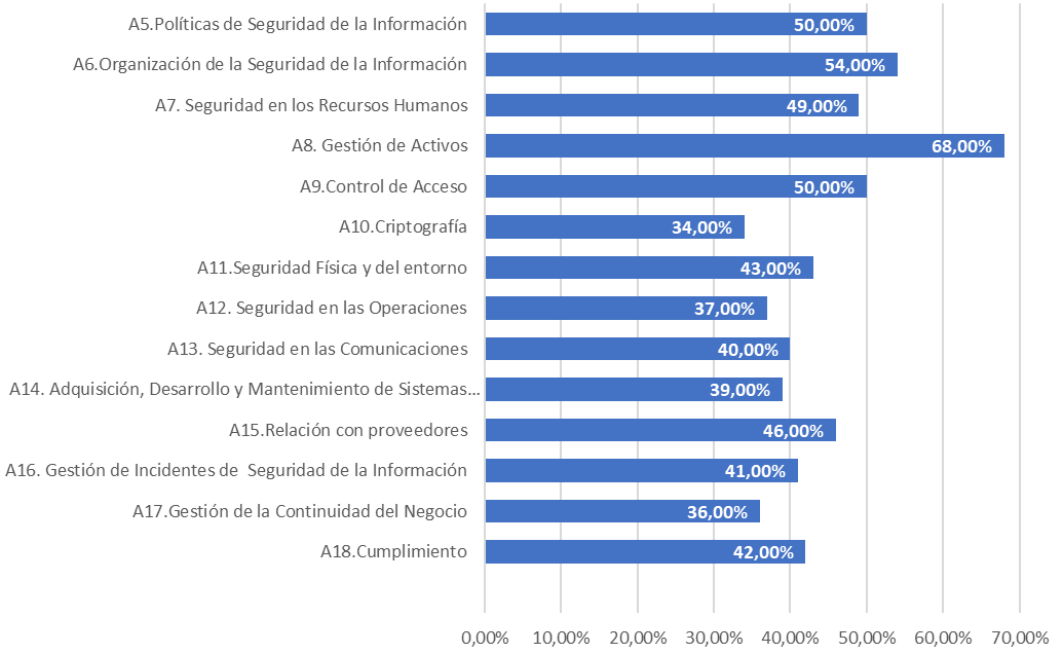


Figura 24. Cumplimiento de los controles posterior a la implementación

Fuente: Autores del Proyecto

Se recomienda a Ultralink implementar lo más pronto posible el presente trabajo ya que al pasar el tiempo los activos que posee la empresa van variando y por ende pueden generarse riesgos que no están contemplados lo cual afectaría el funcionamiento de la empresa.

En el centro de datos se recomienda la implantación de mejores controles físicos y digitales los cuales ayuden a controlar el ingreso no autorizado, también se debe generar para los equipos planes de mantenimiento los cuales ayuden a prevenir daños futuros.

Se recomienda la creación de un departamento encargado de la seguridad de la información el cual debe trabajar en conjunto con todos los gerentes para de esta forma tener una mejor respuesta ante los riesgos a los cuales está expuesto la empresa.

Se debe generar campañas de seguridad de la información las cuales ayudaran a concientizar al personal sobre los riesgos a los cuales están expuestos los activos y la importancia que tiene la seguridad de la información hoy en día.

Es recomendable realizar una actualización periódica de las políticas de seguridad puesto que los activos informáticos que posee la empresa siempre están expuestos a las amenazas humanas, tecnológicas y naturales.

Se recomienda que el personal que va a estar encargado de la implementación del SGSI tenga los conocimientos necesarios para que este sea competente ante las responsabilidades asignadas.

Se debe implementar controles criptográficos los cuales ayuden a proteger la información que se posee en los diferentes tipos de almacenamientos que posee la empresa.

CAPITULO V CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El diseñar un modelo de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001: 2013 ayuda a identificar los diferentes aspectos que debe tener en cuenta una empresa al momento de implementar un modelo de seguridad de la información.

- Permite a las autoridades de Ultralink identificar los riesgos a los cuales está expuesto la empresa, por lo cual luego de una evaluación e implementación de los controles necesarios se pueda controlar estos riesgos y llevarnos a un nivel aceptable para la empresa.

- Para la recopilación de la información sobre los niveles de seguridad según la norma ISO 27001 se procedió a realizar entrevistas al personal del área de tecnología con lo cual se pudo identificar cuáles son los controles presentes en la empresa y de esta forma poder establecer los procesos adecuados que ayuden a mitigar las vulnerabilidades a las cuales está expuesta Ultralink.

- Para la evaluación de los activos que posee la empresa se procedió a utilizar el catálogo de elementos que posee MAGERIT el cual nos proporciona una guía de como ir clasificando los activos y su posterior valoración mediante los criterios acordados con la empresa. Estos criterios de valoración se tuvieron en cuenta tanto en la valoración del impacto, la probabilidad de ocurrencia, el tratamiento de los riesgos y el riesgo residual.

- Para la generación del informe que se le presento a la empresa se desarrolló un resumen ejecutivo en el cual se indicó cuáles fueron las acciones que se realizó para la valoración de los activos, la

identificación de las amenazas y vulnerabilidades, la selección de los controles y la generación de las políticas de seguridad.

- Para la reducción de los riesgos a los cuales están expuestos los activos de la empresa se procedió a implementar la matriz de calor la cual nos ayudan a representar de forma gráfica las zonas en las cuales se encuentran los riesgos de acuerdo con su impacto y probabilidad de ocurrencia se procedió a designar las acciones correctivas según la prioridad del riesgo.

- También se procedió a implementar los controles del ANEXO A de la ISO 27001 los cuales son una guía muy importante al momento de generar las políticas de seguridad de la empresa ya que con estos se busca mejorar la seguridad de la información que se posee.

- Todas las políticas, procedimientos y controles de seguridad que se quieran implementar en Ultralink deben tener el apoyo de la dirección ya que ellos serán los que velen por el correcto funcionamiento de estas.

5.2. Recomendaciones

- Se recomienda utilizar el presente trabajo como referencia para el análisis de las amenazas y vulnerabilidades a las cuales puede estar expuesta una Pyme, la finalidad de esto es que los nuevos trabajos que se desarrollen en esta línea de investigación puedan evolucionar en los métodos de análisis y recolección de datos.

- Es recomendable tener en cuenta las actualizaciones de la ISO 27001 por lo que los controles del Anexo A que se implementaron en el presente trabajo pueden ser diferentes para futuras implementaciones.

- Para futuras implementaciones de sistemas de seguridad basados en la ISO 27001 se recomienda utilizar el Anexo A para la determinación de los niveles de madurez que posee la empresa, ya que este nos

permite realizar un análisis general de todos los dominios de seguridad.

- Finalmente, para la generación de las políticas, procedimientos y controles de seguridad que se quieran implementar en una Pyme se deben tener el apoyo de la dirección ya que ellos serán los que velen por el correcto funcionamiento de estas.

BIBLIOGRAFÍA

[1] “pirani,” 2014. [En línea]. Available: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla. [Último acceso: 20 10 2021].

[2] “SGSI,” 04 12 2013. [En línea]. Available: https://www.pmg-ssi.com/tag/seguridad-de-la-informacion/page/17/. [Último acceso: 30 10 2021].

[3] “ISOTools,” 11 03 2021. [En línea]. Available: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/. [Último acceso: 10 11 2021].

[4] “GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN,” 04 2020. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf. [Último acceso: 16 11 2021].

[5] “ISO27001,” [En línea]. Available: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/. [Último acceso: 17 11 2021].

[6] “ISO27000.ES,” [En línea]. Available: https://www.iso27000.es/iso27000.html. [Último acceso: 16 11 2021].

[7] “repositorio.ug.edu.ec,” 2016. [En línea]. Available: http://repositorio.ug.edu.ec/bitstream/redug/13236/1/TESIS%20DE%20GRADO.pdf. [Último acceso: 02 11 2021].

[8] “ISO27000.ES,” [En línea]. Available: https://www.iso27000.es/sgsi.html. [Último acceso: 17 11 2021].

[9] “INCIBE,” [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf. [Último acceso: 01 11 2021].

[10] J. Bernal, “PDCA HOME,” 23 08 2013. [En línea]. Available: https://www.pdcahome.com/5202/ciclo-pdca/. [Último acceso: 18 11 2021].

[11] G. d. España, “ISO/IRC 27001: PDCA,” [En línea]. Available: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html. [Último acceso: 18 11 2021].

[12] H. Alemán y C. Rodríguez, “Metodologías Para el Análisis de Riesgos en los SGSi,” [En línea]. Available:

https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874. [Último acceso: 22 11 2021].

[13] "MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información," [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 22 11 2021].

[14] C. Alberts, S. Behrens, R. Pethia y W. William, "Carnegie Mellon University," 09 1999. [En línea]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473. [Último acceso: 23 11 2021].

[15] "GlobalSuiteSolutions," 13 07 2020. [En línea]. Available: https://www.globalsuitesolutions.com/es/metodos-de-evaluacion-de-riesgos/. [Último acceso: 12 11 2021].

[16] J. Ruge, "Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica," 2011. [En línea]. Available: http://polux.unipiloto.edu.co:8080/00000744.pdf. [Último acceso: 23 11 2021].

[17] "Un blog editado por ISOTools Excellence," 31 01 2014. [En línea]. Available: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/. [Último acceso: 30 12 2021].

[18] H. Alemán y C. Rodríguez, "Metodologías Para el Análisis de Riesgos en los SGSI," 16 05 2014. [En línea]. Available: https://www.researchgate.net/publication/317149870_Metodologias_para_el_analisis_de_riesgos_en_los_sgsi/fulltext/59281741aca27295a804af42/Metodologias-para-el-analisis-de-riesgos-en-los-sgsi.pdf. [Último acceso: 23 11 2021].

[19] D. d. C. y. Tecnología, "Análisis Comparativo: Metodologías de análisis de riesgos," [En línea]. Available: https://dsi.face.ubiobio.cl/sbravo/1-AUDINF/Comp%20Met%20An-Riesg.pdf. [Último acceso: 10 01 2022].

[20] J. Miranda, "dspace.ups.edu.ec," 10 2020. [En línea]. Available: http://45.235.142.11/assets/uploads/f_trabajos/ante_049866426/Anteproyecto%20Joan%20Miranda%20Jim%C3%83%C2%A9nez%20(1).pdf. [Último acceso: 10 01 2022].

[21] "welivesecurity," 14 05 2013. [En línea]. Available: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/. [Último acceso: 11 06 2022].

[22] "Seguridad de la Información," 16 03 2015. [En línea]. Available: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/#:~:text=Si%20hablamos%20de%20Gesti%C3%B3n%20global,la

s%20fases%20de%20tipo%20log%C3%ADstico.. [Último acceso: 24 04 2022].

[23] “GlobalSUITE SOLUTIONS,” 2021. [En línea]. Available: https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/. [Último acceso: 23 11 2021].

[24] “Ambit Buiding solutions toguether,” 02 06 2020. [En línea]. Available: https://www.ambit-bst.com/blog/metodolog%C3%ADa-itil-gesti%C3%B3n-de-incidencias-y-objetivos. [Último acceso: 23 11 2021].

[25] P. Cichonski, T. Millar, T. Grance y K. Scarfone, Computer Security Incident Handling Guide, Washinton, 2012.

[26] “SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información,” 02 05 2014. [En línea]. Available: https://www.pmg-ssi.com/2014/05/iso-27035-gestion-de-incidentes-de-seguridad-de-la-informacion/. [Último acceso: 24 11 2021].

[27] “ULTRALINK más internet, más velocidad,” 2020. [En línea]. Available: https://ultralink.ec/la-empresa/. [Último acceso: 25 11 2021].

[28] “BANCO PICHINCHA,” 07 05 2021. [En línea]. Available: https://inicio.pichincha.com/portal/blog/post/clasificacion-empresas-por-tamano. [Último acceso: 29 11 2021].

[29] “LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS,” 17 04 2002. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf. [Último acceso: 07 12 2021].

[30] “Telecomunicaciones.gob.ec,” 26 05 2021. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf. [Último acceso: 07 12 2021].

[31] “Defensa.gob.ec,” 17 02 2021. [En línea]. Available: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf. [Último acceso: 07 12 2021].

[32] P. e. I. d. l. A. E. Dirección General de Modernización Administrativa, “administracionelectronica.gob.es,” 10 2012. [En línea]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Último acceso: 12 01 2022].

[33] P. e. I. d. l. A. E. Dirección General de Modernización Administrativa, “administracionelectronica.gob.es,” 10 2012. [En línea]. Available:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 12 01 2022].

[34] “Bibdigital.epn.edu.ec,” 07 2014. [En línea]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/8125/4/CD-5707.pdf. [Último acceso: 24 01 2022].

[35] C. Guzman, “alejandria.poligran.edu.co,” 2015. [En línea]. Available: https://alejandria.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y. [Último acceso: 31 01 2021].

[36] V. Enríquez y P. Torres, “bibdigital.epn.edu.ec,” 07 2014. [En línea]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/8125/4/CD-5707.pdf. [Último acceso: 01 02 2022].

[37] “ISO27000,” 10 2013. [En línea]. Available: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf. [Último acceso: 07 02 2022].

[38] “SCRIBD,” [En línea]. Available: https://es.scribd.com/doc/232787821/ISO27001-2013-Anexo-a-En-Tabla-Excel. [Último acceso: 07 02 2022].

[39] “ISO27001,” [En línea]. Available: https://normaiso27001.es/. [Último acceso: 07 02 2022].

[40] “sig.mineducacion.gov.co,” [En línea]. Available: https://sig.mineducacion.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaWkt5ZlYzcGlHa2. [Último acceso: 22 02 2022].

[41] “UNE.ORG,” 05 2017. [En línea]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj0kYrM5ZT2AhU7RjABHVTaA4oQFnoECAMQAQ&url=https%3A%2F%2Fstatic.eoi.es%2Finline%2Fune-en_iso-iec_27002_norma_mincotur.pdf&usg=AOvVaw3XJmACYf9Ao6ohy9xUjMDo. [Último acceso: 22 02 2022].

[42] “Correos del Ecuador,” 2015. [En línea]. Available: https://www.correosdelecuador.gob.ec/wp-content/uploads/downloads/2015/05/LEY_DE_PROPIEDAD_INTELECTUAL.pdf. [Último acceso: 07 12 2021].

[43] “Ingeniería, Servicios y Comunicaciones,” 07 2019. [En línea]. Available: https://www.isc.cl/wp-content/uploads/2020/04/MANUAL-DE-

POLI%CC%81TICAS-DE-SEGURIDAD-DE-LA-INFORMACIO%CC%81N-DE-ISC.pdf. [Último acceso: 23 02 2022].

[44] “INCIBE,” [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-recursos-humanos.pdf. [Último acceso: 23 02 2022].

[45] “SENAME,” 19 12 2019. [En línea]. Available: https://www.sename.cl/web/wp-content/uploads/2016/11/SGSI-2019/SGSI-PO-14%20POLITICA-DE-CONTROLES-CRIPTOGRAFICOS.pdf. [Último acceso: 03 03 2022].

[46] “sig.mineducacion.gov.co,” [En línea]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj896GR6ar2AhUoQjABHVEKDVcQFnoECAYQAQ&url=https%3A%2F%2Fsig.mineducacion.gov.co%2Flib%2Fdownload.php%3Fnivel1%3Da054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFB. [Último acceso: 03 03 2022].

[47] “ISO27001,” [En línea]. Available: https://normaiso27001.es/a12-seguridad-de-las-operaciones/. [Último acceso: 05 03 2022].

[48] “Mineducacion.gov.co,” [En línea]. Available: https://www.mineducacion.gov.co/1759/articles-349495_recurso_105.pdf. [Último acceso: 06 03 2022].

[49] “www.mtt.gob.cl,” 12 2017. [En línea]. Available: https://www.mtt.gob.cl/wp-content/uploads/2018/12/Pol-SSI-13_v1.0_-_Poli%CC%81tica_de_Seguridad_en_las_Telecomunicaciones.pdf. [Último acceso: 06 03 2022].

[50] “SERNAC,” 11 11 2019. [En línea]. Available: https://www.sernac.cl/portal/617/articles-55451_recurso_4.pdf. [Último acceso: 07 03 2022].

[51] “idiger.gov.co,” 24 05 2019. [En línea]. Available: https://www.idiger.gov.co/documents/20182/325216/Pol%C3%ADtica+Escritorio+Limpio+v1+16-07-2018+%281%29.pdf/12844f87-5cda-4941-80ac-eaabfd6d7f46. [Último acceso: 07 03 2022].

[52] “INCIBE,” [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/buenas_practicas_rrss.pdf. [Último acceso: 08 03 2022].

[53] “mineducacion.gov.co,” [En línea]. Available: https://www.mineducacion.gov.co/1780/articles-407695_galeria_13.pdf. [Último acceso: 08 03 2022].

[54] “ISO27001,” [En línea]. Available: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/. [Último acceso: 08 03 2022].

ANEXOS

Anexo 1. Documentos de la empresa

FILOSOFÍA EMPRESARIAL

SIGNAL TELECOM

MISION

Generamos valor a la sociedad, clientes y todos los grupos de interés, con una gestión innovadora, eficiente, y de calidad en la prestación de servicios de telecomunicaciones, a través del compromiso y experiencia de nuestro equipo de colaboradores.

VISION

Líder ecuatoriano en servicios integrales de Telecomunicaciones, contribuyendo de forma positiva a la sociedad.

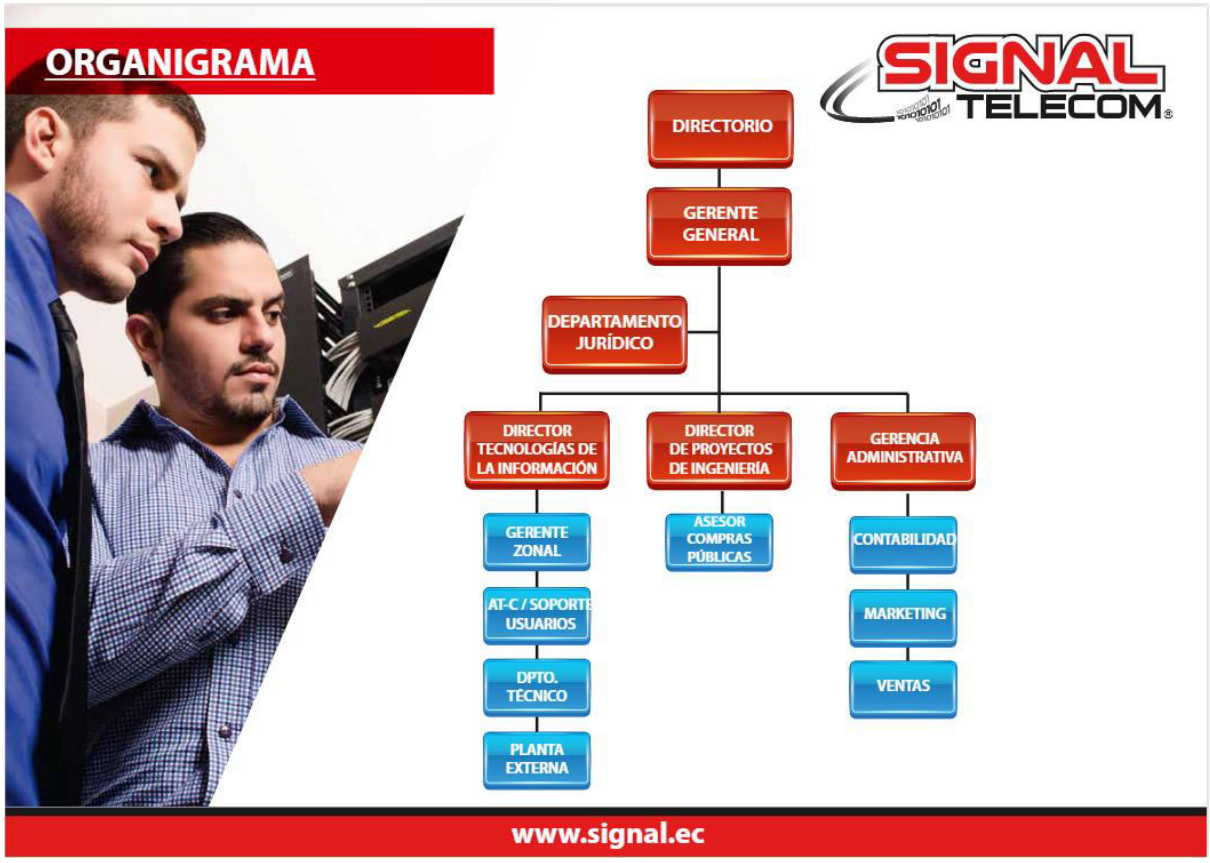
www.signal.ec

COBERTURA

SIGNAL TELECOM

COBERTURA Y SOPORTE TÉCNICO EN TODO EL PAÍS

www.signal.ec


ORGANIGRAMA
SIGNAL TELECOM
DIRECTORIO
GERENTE GENERAL
DEPARTAMENTO JURÍDICO
DIRECTOR TECNOLOGÍAS DE LA INFORMACIÓN
DIRECTOR DE PROYECTOS DE INGENIERÍA
GERENCIA ADMINISTRATIVA
GERENTE ZONAL
AT-C / SOPORTE USUARIOS
DPTO. TÉCNICO
PLANTA EXTERNA
ASESOR COMPRAS PÚBLICAS
CONTABILIDAD
MARKETING
VENTAS
www.signal.ec


SERVICIOS
SIGNAL TELECOM
INTEGRADORES DE SERVICIOS
INTERNET
SEGURIDAD INFORMÁTICA
VOIP
CCTV
www.signal.ec


CLIENTES
SIGNAL TELECOM
Alcaldía CAYAMBE es mi pasión! GAD CAYAMBE
Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE OTAVALO
ALCALDÍA OTAVALO ADMINISTRACIÓN 2014 - 2019
REYBANPAC REY BANANO DEL PACIFICO C.A.
MEP EMPRESA PÚBLICA DE MOVILIDAD MOVIDELNOR EP
Mantahost Hotel
Pastaza cantón GAD MUNICIPAL
Gobierno A. D. Municipal del Cantón Mejía Administración 2014 - 2019
Mejía Crece Contigo
Cruz Roja Ecuatoriana
QUITO ALCALDÍA
GAD AMBATO emapa ep
www.signal.ec


Dirección: Calle Juan León Mera N1-08 y Simón Bolívar
Código Postal 170808 / Quito - Ecuador
PBX: (593) 2-2788-186 / (593) 997 223 230 / (593) 998 000 723
E-mail: isalas@signal.ec
SIGNAL TELECOM®
www.signal.ec

Anexo 2. Test de cumplimiento normativa ISO 27001

4	La Organización y su Contexto	Puntuación	Análisis
4.1	**Entendiendo la Organización y su contexto**		
1.-	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	3	Si
2.-	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	2	Si
3.-	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	1	No
4.2	**Expectativas de las partes interesadas**		
1.-	¿Se han identificado las partes interesadas?	2	Si
2.-	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	2	Si
3.-	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	0	No
4.3	**Alcance del SGSI**		
1.-	¿Se ha determinado el alcance del SGS y se conserva información documentada?	1	No
4.4	**SGS Sistema de Gestión de la Seguridad de la información**		
1.-	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	0	No
5	**Liderazgo**		
5.1	**Liderazgo y compromiso**		
1.-	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	1	No
2.-	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	2	Si
3.-	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	0	No
5.2	**Política de la Seguridad de la Información**		
1.-	¿Se ha definido una Política de la Seguridad de la Información?	1	No
2.-	¿Se ha establecido un marco que permita el establecimiento	1	No

	de objetivos?		
3.-	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda laempresa?	0	No
4.-	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	0	No
5.3	**Roles y Responsabilidades**		
1.-	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	1	No
2.-	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	2	Si
6	**Planificación**		
6.1	**Tratamiento de Riesgos y Oportunidades**		
1.-	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?	1	No
2.-	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	0	No
3.-	¿Se ha definido un proceso de tratamiento de riesgos?	0	No
4.-	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?	0	No
5.-	¿Se mantiene información documentada de los puntos anteriores?	1	No
6.2	**Planificación para consecución de objetivos**		
1.-	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivosdel negocio?	2	Si
2.-	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación	1	No
3.-	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de laorganización teniendo en cuenta las funciones principales dentro de la Organización?	0	No
7	**Soporte**		
7.1	**Recursos**		
1.-	¿Se identifican y asignan los recursos necesarios para el SGSI?	0	No
7.2	**Competencia**		
1.-	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúantareas que puedan afectar a la seguridad?	2	Si

2.-	¿Se mantiene información actualizada sobre la competencia del personal?	2	Si
7.3	**Concienciación**		
1.-	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?	1	No
2.-	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad dela Información?	1	No
7.4	**Comunicación**		
1.-	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	2	Si
2.-	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de laInformación?	1	No
7.5	**Información Documentada**		
1.-	¿Se dispone de la documentación requerida por la norma más la requerida por la organizaciónincluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa(instrucciones técnicas etc.)	0	No
2.-	¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección	0	No
3.-	¿Se controlan los documentos de origen externo?	3	Si
8	**Operación**		
8.1	**Control Operacional**		
1.-	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?	1	No
2.-	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizarcambios en el Sistema de Gestión o procesos de Seguridad?	0	No
3.-	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información antecambios realizados?	0	No
4.-	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad dela Información?	0	No

8.2	**Análisis de riesgos de la Seguridad de la Información**		
1.-	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia	0	No
8.3	**Tratamiento de riesgos de la Seguridad de la Información**		
1.-	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados	0	No
2.-	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?	1	No
3.-	¿Se documenta el nivel de aplicación de todos los controles a aplicar?	1	No
9	**Evaluación del desempeño**		
9.1	**Seguimiento y medición**		
1.-	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?	0	No
2.-	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?	0	No
9.2	**Auditorías Internas**		
1.-	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?	0	No
2.-	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	0	No
3.-	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?	0	No
9.3	**Informe de Revisión por la Dirección**		
1.-	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	0	No
2.-	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?	0	No
10	**Mejora**		

10.1	**No Conformidades y acciones correctivas**		
1.-	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y sutratamiento?	1	No
2.-	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?	0	No
10.2	**Mejora continua**		
1.-	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades demejora?	0	No

Anexo 3. Test de cumplimiento controles ISO 27001

Cláusula	ANEXO A ISO 27001	Puntuación	Análisis
A5	**Políticas de Seguridad de la Información**	1	
A5.1	**Dirección de gestión para la seguridad de la información**	1	
1.-	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordarcon los requisitos del negocio?	1	No
2.-	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	1	No
A6	**Organización de la Seguridad de la Información**	1,25	
A6.1	**Tratamiento de Riesgos y Oportunidades**	1	
1.-	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en lasdistintas tareas o actividades de la organización?	1	No
2.-	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información paraevitar usos o accesos indebidos?	2	Si
3.-	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	0	No
4.-	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadascon la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	1	No
5.-	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?	1	No

A6.2	**Dispositivos Móviles y Teletrabajo**	1,5	
1.-	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	2	Si
2.-	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?	1	No
A7	**Seguridad en los Recursos Humanos**	0,94	
A7.1	**Antes de contratar a un empleado**	1,5	
1.-	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titulación -Referencias	3	Si
2.-	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?	0	No
A7.2	**Durante el contrato**	0,33	
1.-	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?	1	No
2.-	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?	0	No
3.-	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?	0	No
A7.3	**Terminación del contrato**	1	
1.-	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?	0	No
2.-	¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?	2	Si
A8	**Gestión de Activos**	2,06	
A8.1	**Responsabilidad sobre los Activos**	2,5	
1.-	¿Se ha realizado un inventario de activos que dan soporte al negocio y de Información?	3	Si
2.-	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	3	Si
3.-	¿Se han establecido normas para el uso de activos en relación a su seguridad?	3	Si
4.-	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?	1	No

A8.2	**Clasificación de la Información**	2	
1.-	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecermedidas de seguridad especificas?	2	Si
2.-	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidado su nivel de clasificación?	2	Si
3.-	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	2	Si
A8.3	**Manipulación de Soportes**	1,67	
1.-	¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado -Etc.	1	No
2.-	¿Existen procedimientos establecidos para la eliminación de soportes?	3	Si
3.-	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado etc.	1	No
A9	**Control de Acceso**	1	
A9.1	**Requisitos generales para el control de acceso**	0,5	
1.-	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?	1	No
2.-	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?	0	No
A9.2	**Accesos de Usuario**	1,5	
1.-	¿Existen procesos formales de registros de usuarios?	3	Si
2.-	¿Existen procesos formales para asignación de perfiles de acceso?	2	Si
3.-	¿Se define un proceso específico para la asignación y autorización de permisos especiales deadministración de accesos?	2	Si
4.-	¿Se ha establecido una política específica para el manejo de información clasificada como secreto? en cuanto a: -Autenticación -Compromisos	0	No
5.-	¿Se establecen periodos concretos para renovación de permisos de acceso?	1	No
6.-	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad,	1	No

	puesto de trabajo o cese de contratos?		
A9.3	**Responsabilidades de los usuarios**	1	
1.-	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?	1	No
A9.4	**Control de acceso a sistemas y aplicaciones**	1	
1.-	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?	2	Si
2.-	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?	1	No
3.-	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?	0	No
4.-	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración conperfiles bajos de Seguridad?	0	No
5.-	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?	2	Si
A10	**Criptografía**	0	
A10.1	**Control criptográfico**	0	
1.-	¿Existe una política para el establecimiento u yo de controles criptográficos?	0	No
2.-	¿Existe un control del ciclo de vida de las claves criptográficas?	0	No
A11	**Seguridad Física y del entorno**	0,56	
A11.1	**Áreas de Seguridad**	0	
1.-	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?	0	No
2.-	¿Existen controles de acceso a personas autorizadas en áreas restringidas?	0	No
3.-	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información depantallas etc. en áreas de accesibles a personal externo?	0	No
4.-	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?	0	No
5.-	¿Se controlan las áreas de Carga y descarga con procedimientos de control de mercancías entregadas etc.?	0	No
A11.2	**Seguridad de los equipos**	1,11	
	¿Se protegen los equipos tanto del medioambiente	1	No

1.-	como de accesos no autorizados?		
2.-	¿Se protegen los equipos contra fallos de suministro de energía?	2	Si
3.-	¿Existen protecciones para los cableados de energía y de datos?	2	Si
4.-	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?	1	No
5.-	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. ¿Que puedan contener información?	2	Si
6.-	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?	2	Si
7.-	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o vana ser reutilizados?	0	No
8.-	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan elpuesto de trabajo?	0	No
9.-	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?	0	No
A12	**Seguridad en las Operaciones**	0,19	
A12.1	**Procedimientos y responsabilidades**	0,8	
1.-	¿Se documentan los procedimientos y se establecen responsabilidades?	0	No
2.-	¿Se controla que la información sobre procedimientos se mantenga actualizada?	0	No
3.-	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?	0	No
4.-	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?	2	Si
5.-	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	2	Si
A12.2	**Protección contra software malicioso**	0	
1.-	¿Existen sistemas de detección para Software malicioso o malware?	0	No
A12.3	**Copias de Seguridad**	0	
1.-	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?	2	Si
A12.4	**Registros y supervisión**	0,5	
1.-	¿Se realiza un registro de eventos? -Intentos de acceso fallidos/exitosos -Desconexiones del sistema	1	No

	-Alertas de fallos Etc.		
2.-	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?	0	No
3.-	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?	1	No
4.-	¿Existe un control de sincronización de los distintos sistemas?	0	No
A12.5	**Control del Software**	0	
1.-	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?	0	No
A12.6	**Vulnerabilidad Técnica**	0	
1.-	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?	0	No
2.-	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?	0	No
A12.6	**Auditorias de Sistemas de Información**	0	
1.-	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?	0	No
2.-	¿Se establecen protocolos específicos para desarrollo de auditorías Software considerando su impacto en los sistemas?	0	No
A13	**Seguridad en las Comunicaciones**	0,38	
A13.1	**Seguridad de Redes**	0	
1.-	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?	0	No
2.-	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?	0	No
3.-	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?	0	No
A13.2	**Intercambio de Información**	0,75	
1.-	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?	1	No
2.-	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?	0	No
3.-	¿Se establecen normas o criterios de seguridad en mensajería electrónica?	2	Si
4.-	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades	0	No
A14	**Adquisición, desarrollo y**	0,31	

	mantenimiento de sistemas de información		
A14.1	**Intercambio de Información**	0,5	
1.-	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemasde Información?	0	No
2.-	¿Se especifican los requisitos de Seguridad de la información en el diseño de nuevos sistemas?	0	No
3.-	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?	1	No
4.-	¿Se establecen medidas de protección para transacciones Online?	1	No
A14.2	**Seguridad en los procesos de Soporte**	0,44	
1.-	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?	0	No
2.-	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?	0	No
3.-	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?	2	Si
4.-	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?	0	No
5.-	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?	0	No
6.-	¿Se realiza una evaluación de riesgos para herramientas de desarrollo de Software?	0	No
7.-	¿Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros?	0	No
8.-	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?	2	Si
9.-	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?	0	No
A14.3	**Datos de prueba**	0	
1.-	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?	0	No
A15	**Relación con Proveedores**	0,75	
A15.1	**Seguridad en la Relación con Proveedores**	1	
1.-	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?	0	No
2.-	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?	2	Si
3.-	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro?	1	No
A15.1	**Gestión de servicios externos**	0,5	
1.-	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?	0	No

2.-	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?	1	No
A16	**Gestión de incidentes de seguridad de lainformación**	0,43	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**	0,43	
1.-	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?	2	Si
2.-	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad dela Información?	1	No
3.-	¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	0	No
4.-	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?	0	No
5.-	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?	0	No
6.-	¿La información que proporcionada por los eventos en la Seguridad de la información son tratadospara tomar medidas preventivas?	0	No
7.-	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de laInformación?	0	No
A17	**Gestión de la Continuidad del Negocio**	0,17	
A17.1	**Continuidad de la seguridad de la información.**	0,3333333	
1.-	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?	1	No
2.-	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad delNegocio?	0	No
3.-	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?	0	No
A17.2	**Redundancias**	0	
1.-	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?	0	No
A18	**Cumplimiento**	0,5	
A18.1	**Cumplimiento de los requisitos legales y contractuales.**	1	
1.-	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento? -LOPD -Leyes para comercio Electrónico -Transacciones Bancarias -Información Protegida -Otras propias del negocio o actividad -Ley general de Telecomunicaciones	2	Si

2.-	¿Existen procedimientos implementados sobre la propiedad intelectual?	1	No
3.-	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	2	Si
4.-	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	0	No
5.-	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	0	No
A18.2	**Revisiones de la Seguridad de la Información**	0	
1.-	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?	0	No
2.-	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?	0	No
3.-	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protecciónpara la seguridad de la información?	0	No

Anexo 4. Identificación de incidentes

Tipo de incidentes	**Ocurrencia**	
	Si/No	**Frecuencia**
Cuentas de usuarios o credenciales vulneradas.	Si	Rara vez
Acceso físico a información no autorizada.	No	Nunca
Intrusión física a áreas no autorizadas.	No	Nunca
Destrucción de información no autorizada	No	Nunca
Correo electrónico masivo con contenido sospechoso o no deseado.	Si	Frecuentemente
Uso de cualquier medio de la organización para acosar o divulgar información confidencial.	No	Nunca
Ingreso a contenido inadecuado por parte del personal por cualquier medio.	No	Nunca
Sistema, de la infraestructura tecnológica infectado aplicación o componente.	Si	Frecuentemente
Modificación, instalación o eliminación no autorizada de software	Si	Rara Vez
Sabotaje físico o daños que atenten a los activos de información que posee.	Si	Rara Vez cortan la fibra óptica

Interrupción en la disponibilidad del servicio (Condiciones ajenas o desastres naturales)	Si	Rara Vez caída de postes, rotura de fibra, deslaves, caída de árboles, viento
Robo de información por exponer a terceros información confidencial.	No	Nunca
Pérdida de información por descuido del personal. (Abandono o descuido del puesto de trabajo)	Si	Rara Vez se quemó un computador y no lo respaldaron en la nube
Abuso de privilegios o de políticas de seguridad de la información.	No	Nunca
Divulgación de información no autorizada a ser compartida con ciertos usuarios.	No	Nunca
Mal uso de la información, para actividades que no están dentro del ámbito laboral.	Si	Rara Vez
Falla en la red (por tráfico inusual)	No	Nunca
Servicios accesibles fácilmente porque presentan criptografía débil	Si	Frecuentemente
Suplantación de identidad para obtener beneficios ilegítimos	No	Nunca
Modificación no autorizada de la información por parte de un atacante empleando credenciales sustraídas de un sistema o aplicación (Ransomware)	No	Nunca
Ingresar o ejecutar código malicioso para dañar el sistema o dañar al sistema. (Malware)	No	Nunca
Infracciones de derechos de autor o piratería	No	Nunca
Pérdida o robo de equipos por exponer información confidencial que estos contienen.	No	Nunca
Daños o cambios físicos no autorizados a los sistemas	No	Nunca

Anexo 5. Inventario de activos

Activos Físicos

PC de escritorio y laptops

COD	Área	Equipo	Detalles del Equipo				Ubicación	Responsable	Características	CUSTODIO
			Marca	Modelo	Procesador	Memoria				
AF01	Departamento técnico	Laptop	ASUS	X441UAK	I7 7500U	4 GIGAS	Departamento técnico	Departamento técnico	Windows 10 pro de 64 bits	Víctor Erazo
AF02	Departamento técnico	Laptop	DELL	PowerEdge R230	Intel Xeon	16 GIGAS	Departamento técnico	Departamento técnico	Windows 10 pro de 64 bits	Santiago Llumiquinga
AF03	Departamento técnico	Laptop					Departamento técnico	Departamento técnico	Windows 10 pro de 64 bits	Roberto San
AF04	Departamento administrativo	DELL NUC	ASUS	9560NGW	Intel Celeron N4000	4 GIGAS	Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Gabriela Sani
AF05	Departamento administrativo	DELL NUC	ASUS	9560NGW	Intel Celeron N4000	4 GIGAS	Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Cristina Guerron
AF06	Departamento administrativo	DELL NUC	ASUS	9560NGW	Intel Celeron N4000	4 GIGAS	Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Melanyn Tamay
AF07	Departamento administrativo	DELL NUC	ASUS	9560NGW	Intel Celeron N4000	4 GIGAS	Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Damaris Peña
AF08	Departamento administrativo	DELL NUC	ASUS	9560NGW	Intel Celeron N4000	4 GIGAS	Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Carla Noroña

AF09	Departamento administrativo	Laptop					Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Nataly Javas
AF10	Departamento administrativo	Pc escritorio					Departamento administrativo	Departamento administrativo	Windows 10 pro de 64 bits	Andrés Tobar
AF11	Gerencia	Laptop					Gerencia	Gerencia	Windows 10 pro de 64 bits	Inés Flores
AF12	Gerencia	Laptop					Gerencia	Gerencia	Windows 10 pro de 64 bits	Iván Salas

Servidores

COD	Área	Marca	Modelo	Procesador	Memoria	Serie	Características	Ubicación	Responsable	Custodio
AF13	Cetro de datos	DELL	R240	Intel Xeon	16 GIGAS	2236-AC	S.O GGC	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga
AF14	Cetro de datos	DELL	R240	Intel Xeon	16 GIGAS	2236-AC	S.O GGC	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga
AF15	Cetro de datos	DELL	R240	Intel Xeon	16 GIGAS	2236-AC	S.O GGC	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga
AF16	Cetro de datos	DELL	R240	Intel Xeon	16 GIGAS	2236-AC	S.O GGC	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga
AF17	Cetro de datos	DELL	PowerEdge R230	Intel Xeon	16 GIGAS	E3-1220	Windows 10 internamente máquinas virtuales BMware	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga
AF18	Cetro de datos	DELL	PowerEdge R230	Intel Xeon	16 GIGAS	E3-1220	Ubuntu server	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga

AF19	Centro de datos	DELL	PowerEdge R230	Intel Xeon	16 GIGAS	E3-1220	Ubuntu server	Centro de datos	Santiago Llumiquinga	Santiago Llumiquinga

Firewall

COD	Área	Marca	Modelo	Versión	Ubicación	Responsable	Observaciones
AF20	Centro de datos	N/A	N/A	N/A	Centro de datos	Santiago Llumiquinga	Configuración interna en cada router

Switch y Routers

COD	Área	Equipo	Detalles del Equipo			Ubicación	Responsable	Características
			Marca	Modelo	Serie			
AF21	Centro de datos	Router	MIKROTIK	CCR1072-1G-8S+	727306C33F	Centro de datos	Santiago Llumiquinga	
AF22	Centro de datos	Router	MIKROTIK	CCR1072-1G-8S+	D8420C26D867	Centro de datos	Santiago Llumiquinga	
AF23	Centro de datos	Router	MIKROTIK	CCR1072-1G-8S+	D8420E641DDB	Centro de datos	Santiago Llumiquinga	
AF24	Centro de datos	Switch		MA5680T	MA5600V800R015C00	Centro de datos	Santiago Llumiquinga	OLT
AF25	Centro de datos	Switch de CORE	HP Comware	A5820X-2AXG-SFP+	1211P09	Centro de datos	Santiago Llumiquinga	

Activos de software

Software de aplicación

COD	Software	Detalles del Software		Responsable	Características
		Tipo	Costo		
AS01	Sistemas operativos	Windows	Pagado	Santiago Llumiquinga	Licencia original
		Ubuntu server 20.04	No aplica	Santiago Llumiquinga	
AS02	Software de manejo de red	U2000 software de administración de red		Santiago Llumiquinga	Con crack software para manejar olt
AS03	Software de aplicaciones de oficina	Trantor sistema contable	Pagado	Ines Flores (Gerente)	
		Office 2010	Pagado	Santiago Llumiquinga	Laptops licencia original de fabrica DELL NUC original Pc escritorio crack

Activos de información

COD	Tipo	Estado	Criterio	Característica
AI01	Base de datos	Digital	Privado	No aplica
AI02	Documentos compartidos	Digital	Privado	OneDrive, Google drive
AI03	Planillas	Digital	Privado	No aplica
AI04	Información de procesos de contratación	Físico	Privado	Es la documentación legal para la contratación
AI05	Facturas de Pagos	Digital y Físico	Privado	Son las que se genera por los proveedores
AI06	Balances	Digital	Privado	Estadísticas de la empresa
AI07	Ordenes de trabajo	Físico	Privado	No aplica
AI08	Información de servicios	Digital y Físico	Publico	No aplica
AI09	Diagrama de red	Digital y Físico	Privado	No aplica

Activos de Personal

COD	Área	Cantidad
AP01	Departamento técnico	9
AP02	Departamento administrativo	7

AP03	Gerencia	2

Equipamiento auxiliar

Control de Acceso

COD	Marca	Modelo	Tipo
AEA01	N/A	Chapa	Llave

UPS

COD	Marca	Modelo	Serie	Característica
AEA02	XMART PACK	XMA4939	XBU-SW-2.0K-120-NB	Autonomía de 6 horas

Fibra Óptica

COD	DESCRIPCION	MODELO/SERIE
AEA03	Fusionadora FUJIKURA	FSM-41S / 596YM1NR6YLKWVKG
AEA04	Cargador fusionadora	ADC-13
AEA05	Peladora FUJIKURA	SS03
AEA06	Cortadora FUJIKURA	CT50 / 56220
AEA07	OTDR EXFO	MAX7178 / 718355
AEA08	Etiquetadora BRADY	BMP-21PLUS
AEA09	Power Meter más VFL	M1519030345
AEA10	Cargador de OTDR EXFO	EA10953E-240 / 23121005511
AEA11	Fusionadora GREENLEE	910FS / 100695
AEA12	Cortadora SUMITOMO	FC-7
AEA13	PON Power Meter	RY3201 / 02989

Aire acondicionado

COD	Marca	Modelo	Serie
AEA10	LG	PISO TECHO INVERTER Frio Calor	R410A

Activos de Servicios

COD	Servicio	Usuarios
ASE01	Correo electrónico	18

Activos de Instalaciones

COD	Instalaciones	Cantidad	Usuarios
AIN01	Edificios	1	18

AIN02	Vehículos	3	4
AIN03	Antenas	7	N/A

Anexo 6. Valoración de activos

Nombre del Activo	Ubicación	Valoración de la pérdida del activo			
		Confidencialidad	Disponibilidad	Integridad	Total, del impacto
Laptop Asus	Departamento técnico	2	4	2	3
Laptop DELL	Departamento técnico	2	4	2	3
Laptop	Departamento administrativo	3	4	3	3
DELL NUC Asus	Departamento administrativo	3	4	3	3
Pc Escritorio	Gerencia	3	3	3	3
DELL DELL NUC	Gerencia	3	3	3	3
Servidor DELL R240	Centro de datos	4	5	4	4
Servidor DELL PowerEdge R230	Centro de datos	4	5	4	4
Router MIKROTIK	Centro de datos	4	5	4	4
Switch de CORE HP Comware	Centro de datos	4	5	4	4
S.O windows	D. Administrativo D. Técnico Gerencia	2	3	2	3
S.O ubuntu	Centro de datos	3	4	4	4
Sistema contable Trantor	Departamento administrativo	4	4	4	4
Base de datos	Centro de datos	4	5	4	4
Documentos compartidos	D. Administrativo D. Técnico Gerencia	3	3	3	3
Planillas	Departamento administrativo	2	2	2	2
Información de procesos de contratación	Departamento administrativo	2	2	2	2
Facturas de Pagos	Departamento administrativo	3	4	3	3
Balances	Departamento administrativo	3	3	3	3
Ordenes de trabajo	D. Administrativo D. Técnico Gerencia	2	2	2	2
Información de servicios	D. Administrativo D. Técnico Gerencia	2	2	2	2
Diagrama de red	D. Técnico	3	3	3	3

	Gerencia				
UPS XMART PACK	Centro de datos D. Administrativo D. Técnico	1	5	0	2
Fusionadora FUJIKURA	Departamento técnico	1	4	0	1
Cargador fusionadora	Departamento técnico	0	4	0	1
Peladora FUJIKURA	Departamento técnico	0	4	0	1
Cortadora FUJIKURA	Departamento técnico	0	4	0	1
OTDR EXFO	Departamento técnico	0	4	0	1
Etiquetadora BRADY	Departamento técnico	0	4	0	1
Power Meter más VFL	Departamento técnico	0	4	0	1
Aire acondicionado PISO TECHO INVERTER Frio Calor	Centro de datos	0	4	0	1
Correo electrónico	Ninguno	0	4	3	3
Autos	Ninguno	0	3	0	1
Antenas	Ninguno	0	5	4	3

Anexo 7. Matriz de evaluación de amenazas

Nombre del Activo	Vulnerabilidades	Amenazas	Degradación	Probabilidad de la ocurrencia	Justificación
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
PCs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura

	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el	Robo	3	3	No se poseen los equipos correctamente inventariados

	almacenamiento de los equipos				
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios

	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización

	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	Falta de equipamiento para prevención de incendios
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	Equipo de enfriamiento deficiente para la infraestructura
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	Personal poco capacitado
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	No se poseen los equipos correctamente inventariados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	No se controla las personas que pude ingresar a la organización
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	Falta niveles de seguridad en los routers
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	Problemas externos a la organización
S.O Windows	Errores en la configuración de seguridad	Ciberataques	3	3	Puede suceder por mala manipulación de los equipos y falta de seguridad lógica.
	Asignación errada en los accesos	Abuso de los equipos	1	3	No posee una generación correcta de los roles, ni sistemas de control.
	Ausencia de documentación de uso	Modificación sin autorización	4	4	Falta de políticas y personal encargado de generar la documentación. Tampoco tiene una base de conocimiento con soluciones ante problemas

	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	Falta de personal capacitado y capacitación al personal nuevo
	Interfaces de difícil manipulación	Errores de uso	2	3	No existe documentación sobre la manipulación de las herramientas que posee la empresa
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	Falta de concientización del personal
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	Falta de políticas para poder gestionar las contraseñas
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	Falta de políticas de seguridad de la información
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	3	3	Puede suceder por mala manipulación de los equipos y falta de seguridad lógica.
	Asignación errada en los accesos		1	3	No posee una generación correcta de los roles, ni sistemas de control.
	Ausencia de documentación de uso	Modificación sin autorización	4	4	Falta de políticas y personal encargado de generar la documentación. Tampoco tiene una base de conocimiento con soluciones ante problemas
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	Falta de personal capacitado y capacitación al personal nuevo
	Interfaces de difícil manipulación	Errores de uso	2	3	No existe documentación sobre la manipulación de las herramientas que posee la empresa
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	Falta de concientización del personal
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	Falta de políticas para poder gestionar las contraseñas
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	Falta de políticas de seguridad de la información

Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	3	3	Puede suceder por mala manipulación de los equipos y falta de seguridad lógica.
	Asignación errada en los accesos	Abuso de los equipos	1	3	No posee una generación correcta de los roles, ni sistemas de control.
	Ausencia de documentación de uso	Modificación sin autorización	4	4	Falta de políticas y personal encargado de generar la documentación. Tampoco tiene una base de conocimiento con soluciones ante problemas
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	Falta de personal capacitado y capacitación al personal nuevo
	Interfaces de difícil manipulación	Errores de uso	2	3	No existe documentación sobre la manipulación de las herramientas que posee la empresa
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	Falta de concientización del personal
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	Falta de políticas para poder gestionar las contraseñas
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	Falta de políticas de seguridad de la información
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	3	3	Puede suceder por mala manipulación de los equipos y falta de seguridad lógica.
	Asignación errada en los accesos	Abuso de los equipos	1	3	No posee una generación correcta de los roles, ni sistemas de control.
	Ausencia de documentación de uso	Modificación sin autorización	4	4	Falta de políticas y personal encargado de generar la documentación. Tampoco tiene una base de conocimiento con soluciones ante problemas
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	Falta de personal capacitado y capacitación al personal nuevo
	Interfaces de difícil manipulación	Errores de uso	2	3	No existe documentación sobre la manipulación de las herramientas que posee la empresa

	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	Falta de concientización del personal
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	Falta de políticas para poder gestionar las contraseñas
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	Falta de políticas de seguridad de la información
Office 2010	Errores en la configuración de seguridad	Ciberataques	3	3	Puede suceder por mala manipulación de los equipos y falta de seguridad lógica.
	Asignación errada en los accesos	Abuso de los equipos	1	3	No posee una generación correcta de los roles, ni sistemas de control.
	Ausencia de documentación de uso	Modificación sin autorización	4	4	Falta de políticas y personal encargado de generar la documentación. Tampoco tiene una base de conocimiento con soluciones ante problemas
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	Falta de personal capacitado y capacitación al personal nuevo
	Interfaces de difícil manipulación	Errores de uso	2	3	No existe documentación sobre la manipulación de las herramientas que posee la empresa
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	Falta de concientización del personal
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	Falta de políticas para poder gestionar las contraseñas
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	Falta de políticas de seguridad de la información
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	3	2	Falta de controles de seguridad
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	4	3	No existen políticas de seguridad

	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	4	4	No existe una correcta asignación en las responsabilidades
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	3	Existe encargados que realizan varias gestiones que solo ellos las pueden ejecutar
	No existencia de políticas de mensajería	Perdida de los datos	5	4	No existen políticas y control antispam
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	4	No se realiza capacitaciones sobre seguridad
Personal de planta (técnicos, secretarias, contadores, gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	3	2	Falta de controles de seguridad
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	4	3	No existen políticas de seguridad
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	4	4	No existe una correcta asignación en las responsabilidades
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	3	Existe encargados que realizan varias gestiones que solo ellos las pueden ejecutar
	No existencia de políticas de mensajería	Perdida de los datos	5	4	No existen políticas y control antispam
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	4	No se realiza capacitaciones sobre seguridad
Bases de datos	Inadecuada administración de los datos	Fuga de información	4	4	Documentación inexistente

	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	Falta de mantenimiento a las instalaciones
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	2	2	Existe una falta de digitalización de algunos procesos
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	3	2	No existen políticas de continuidad del negocio
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	Falta de presupuesto para el mantenimiento de las instalaciones
	No existencia de copias de respaldo	Perdida de información	4	4	No existen políticas
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	4	4	Documentación inexistente
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	Falta de mantenimiento a las instalaciones
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	2	2	Existe una falta de digitalización de algunos procesos
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	3	2	No existen políticas de continuidad del negocio
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	Falta de presupuesto para el mantenimiento de las instalaciones
	No existencia de copias de respaldo	Perdida de información	4	4	No existen políticas

Balances	Inadecuada administración de los datos	Fuga de información	4	4	Documentación inexistente
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	Falta de mantenimiento a las instalaciones
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	2	2	Existe una falta de digitalización de algunos procesos
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	3	2	No existen políticas de continuidad del negocio
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	Falta de presupuesto para el mantenimiento de las instalaciones
	No existencia de copias de respaldo	Perdida de información	4	4	No existen políticas
Planillas de pago	Falta de protecciones contra incendios	Incendio	2	4	Documentación inexistente
	Falta de instalaciones correctas	Daños por agua	2	3	Falta de mantenimiento a las instalaciones
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	Falta de presupuesto para el mantenimiento de las instalaciones
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	No existen políticas de continuidad del negocio
Planillas de servicios	Falta de protecciones contra incendios	Incendio	2	4	Documentación inexistente
	Falta de instalaciones correctas	Daños por agua	2	3	Falta de mantenimiento a las instalaciones

	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	Falta de presupuesto para el mantenimiento de las instalaciones
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	No existen políticas de continuidad del negocio
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	2	4	Documentación inexistente
	Falta de instalaciones correctas	Daños por agua	2	3	Falta de mantenimiento a las instalaciones
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	Falta de presupuesto para el mantenimiento de las instalaciones
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	No existen políticas de continuidad del negocio
Información de los servicios	Falta de protecciones contra incendios	Incendio	2	4	Documentación inexistente
	Falta de instalaciones correctas	Daños por agua	2	3	Falta de mantenimiento a las instalaciones
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	Falta de presupuesto para el mantenimiento de las instalaciones
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	No existen políticas de continuidad del negocio
Diagramas de red	Falta de protecciones contra incendios	Incendio	2	4	Documentación inexistente
	Falta de instalaciones correctas	Daños por agua	2	4	Falta de mantenimiento a las instalaciones
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	Falta de presupuesto para el mantenimiento de las instalaciones
	Ausencia de políticas para tener un correcto	Robo de documentación	3	3	No existen políticas de continuidad del negocio

	almacenamiento de la documentación				
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	4	Los controles de acceso existentes son básicos
	Ausencia de protecciones digitales	Perdida de equipos	0	3	Existen solo las protecciones físicas
	Ubicación en área susceptible a desastres	Desastres naturales	2	2	Situaciones externas
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	Situaciones externas
	Perdida de información	Destrucción de los equipos	2	2	Irresponsabilidad del personal
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	4	Los controles de acceso existentes son básicos
	Ausencia de protecciones digitales	Perdida de equipos	0	3	Existen solo las protecciones físicas
	Ubicación en área susceptible a desastres	Desastres naturales	2	2	Situaciones externas
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	Situaciones externas
	Perdida de información	Destrucción de los equipos	2	2	Irresponsabilidad del personal
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	4	Los controles de acceso existentes son básicos
	Ausencia de protecciones digitales	Perdida de equipos	0	3	Existen solo las protecciones físicas
	Ubicación en área susceptible a desastres	Desastres naturales	2	2	Situaciones externas
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	Situaciones externas
	Perdida de información	Destrucción de los equipos	2	2	Irresponsabilidad del personal

Correo	Interfaz de usuarios complejas	Error en el uso	0	1	No existe capacitación sobre el uso del correo
	Gestión deficiente de contraseñas	Vulneración de la sesión	2	3	No existe una capacitación sobre la administración correcta de las contraseñas
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	3	No existen políticas
	Líneas de comunicación sin protección	Filtración de información	1	1	No existen protecciones
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	1	1	No existen políticas
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	Falta de presupuesto para realizar el mantenimiento
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	Falta de presupuesto
	Manejo inadecuado de los equipos físics	Destrucción de los equipos	3	3	Falta de capacitación del personal
	Monitoreo inadecuado de las instalaciones	Robo	3	3	Falta de presupuesto
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	Falta de planificación sobre el almacenamiento de los recursos
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	Falta de presupuesto para realizar el mantenimiento
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	Falta de presupuesto
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	Falta de capacitación del personal

	Monitoreo inadecuado de las instalaciones	Robo	3	3	Falta de presupuesto
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	Falta de planificación sobre el almacenamiento de los recursos
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	Falta de presupuesto para realizar el mantenimiento
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	Falta de presupuesto
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	Falta de capacitación del personal
	Monitoreo inadecuado de las instalaciones	Robo	3	3	Falta de presupuesto
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	Falta de planificación sobre el almacenamiento de los recursos
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	Falta de presupuesto para realizar el mantenimiento
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	Falta de presupuesto
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	Falta de capacitación del personal
	Monitoreo inadecuado de las instalaciones	Robo	3	3	Falta de presupuesto
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	Falta de planificación sobre el almacenamiento de los recursos

Anexo 8. Matriz de valoración del impacto de las amenazas en función de CID

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del impacto CID			Valor total del impacto CID	Impacto	Magnitud del impacto			Magnitud total del impacto
			C	I	D			C	I	D	
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	4	9	3	B	M	A	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	4	4	10	3	B	A	A	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	4	5	13	4	A	A	MA	A
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	1	2	5	2	B	MB	B	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	1	1	3	5	2	MB	MB	M	B
	Falta de conexiones seguras	Error en la manipulación de las redes	4	5	3	12	4	A	MA	M	A
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	4	9	3	B	M	A	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	4	4	10	3	B	A	A	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	5	5	14	5	A	A	MA	MA
	No existe medidas adecuadas para el	Robo	2	1	2	5	2	B	MB	B	B

	almacenamiento de los equipos										
	No existe control sobre las personas que ingresan y salen de la organización	Robo	1	1	3	5	2	MB	MB	M	B
	Falta de conexiones seguras	Error en la manipulación de las redes	3	5	3	11	4	A	MA	M	A
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	4	9	3	B	M	A	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	4	4	10	3	B	A	A	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	5	5	14	5	A	A	MA	MA
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	0	1	3	4	1	D	MB	M	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	1	1	3	5	2	MB	MB	M	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	3	5	3	11	4	A	MA	M	A
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	3	4	4	11	4	M	A	A	A
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	1	1	5	7	2	MB	MB	MA	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	2	3	5	10	3	B	M	MA	M
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	4	5	12	4	M	A	MA	A

	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	3	3	10	3	A	M	M	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	5	5	15	5	MA	MA	MA	MA
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	3	4	4	11	4	M	A	A	A
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	1	1	5	7	2	MB	MB	MA	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	2	3	5	10	3	B	M	MA	M
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	4	5	12	4	M	A	MA	A
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	3	3	10	3	A	M	M	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	5	5	15	5	MA	MA	MA	MA
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	2	4	4	10	3	B	A	A	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	1	2	5	8	3	MB	B	MA	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	5	5	15	5	MA	MA	MA	MA
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	3	10	3	A	M	M	M

	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	4	5	12	4	M	A	MA	A
	Falta de conexiones seguras	Error en la manipulación de las redes	5	5	5	15	5	MA	MA	MA	MA
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	1	4	5	10	3	MB	A	MA	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	1	1	5	7	2	MB	MB	MA	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	2	3	5	10	3	B	M	MA	M
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	4	5	12	4	M	A	MA	A
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	3	4	11	4	A	M	M	A
	Falta de conexiones seguras	Error en la manipulación de las redes	5	5	5	15	5	MA	MA	MA	MA
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	5	7	2	MB	MB	MA	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	5	10	3	B	M	MA	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	4	5	12	4	M	A	MA	A
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	3	10	3	A	M	M	M

	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	5	5	15	5	MA	MA	MA	MA
	Falta de conexiones seguras	Error en la manipulación de las redes	4	5	5	14	5	A	MA	MA	MA
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	3	4	5	12	4	M	A	MA	A
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	1	2	5	8	3	MB	B	MA	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	4	5	14	5	A	A	MA	MA
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	5	5	5	15	5	MA	MA	MA	MA
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	5	5	15	5	MA	MA	MA	MA
	Falta de conexiones seguras	Error en la manipulación de las redes	4	5	5	14	5	MA	MA	MA	MA
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	0	0	5	5	2	D	D	MA	B
S.O Windows	Errores en la configuración de seguridad	Ciberataques	5	5	5	15	5	MA	MA	MA	MA
	Asignación errada en los accesos	Abuso de los equipos	4	5	3	12	4	A	MA	M	A
	Ausencia de documentación de uso	Modificación sin autorización	4	5	4	13	4	A	MA	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	5	4	4	13	4	MA	A	A	A
	Interfaces de difícil manipulación	Errores de uso	1	1	4	6	2	MB	MB	A	B

	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	5	3	12	4	A	MA	M	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	5	4	14	5	MA	MA	A	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	1	0	5	6	2	MB	D	MA	B
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	5	5	5	15	5	MA	MA	MA	MA
	Asignación errada en los accesos		4	5	3	12	4	A	MA	M	A
	Ausencia de documentación de uso	Modificación sin autorización	4	5	4	13	4	A	MA	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	5	4	4	13	4	MA	A	A	A
	Interfaces de difícil manipulación	Errores de uso	1	1	4	6	2	MB	MB	A	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	1	5	3	9	3	MB	MA	M	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	5	4	14	5	MA	MA	A	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	1	0	5	6	2	MB	D	MA	B
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	5	5	5	15	5	MA	MA	MA	MA
	Asignación errada en los accesos	Abuso de los equipos	4	5	4	13	4	A	MA	A	A
	Ausencia de documentación de uso	Modificación sin autorización	4	5	4	13	4	A	MA	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	5	4	4	13	4	MA	A	A	A
	Interfaces de difícil manipulación	Errores de uso	1	1	4	6	2	MB	MB	A	B

	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	5	3	12	4	A	MA	M	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	5	4	14	5	MA	MA	A	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	1	0	5	6	2	MB	D	MA	B
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	5	5	5	15	5	MA	MA	MA	MA
	Asignación errada en los accesos	Abuso de los equipos	4	5	4	13	4	A	MA	A	A
	Ausencia de documentación de uso	Modificación sin autorización	4	5	5	14	5	A	MA	MA	MA
	Inadecuada utilización de los sistemas	Errores de mantenimiento	5	4	4	13	4	MA	A	A	A
	Interfaces de difícil manipulación	Errores de uso	1	1	4	6	2	MB	MB	A	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	5	3	12	4	A	MA	M	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	5	4	14	5	MA	MA	A	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	1	0	5	6	2	MB	D	MA	B
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	0	0	0	0	D	D	D	D
	Asignación errada en los accesos	Abuso de los equipos	0	1	0	1	0	D	MB	D	D
	Ausencia de documentación de uso	Modificación sin autorización	4	5	4	13	4	A	MA	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	5	4	4	13	4	MA	A	A	A
	Interfaces de difícil manipulación	Errores de uso	1	1	4	6	2	MB	MB	A	B

	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	5	3	12	4	A	MA	M	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	5	4	14	5	MA	MA	A	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	1	0	5	6	2	MB	D	MA	B
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	4	5	5	14	5	A	MA	MA	MA
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	2	4	3	9	3	B	A	M	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	5	14	5	MA	A	MA	MA
	Entrenamiento insuficiente del personal	Perdida de personal clave	3	3	4	11	4	M	M	A	A
	No existencia de políticas de mensajería	Perdida de los datos	2	3	2	7	2	B	M	B	B
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	5	15	5	MA	MA	MA	MA
Personal de planta (técnicos, secretarias, contadores, gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	4	5	5	14	5	A	MA	MA	MA
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	3	10	3	M	A	M	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	5	14	5	MA	A	MA	MA
	Entrenamiento insuficiente del personal	Perdida de personal clave	3	3	4	11	4	M	M	A	A
	No existencia de políticas de mensajería	Perdida de los datos	4	3	4	11	4	A	M	A	A

	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	5	15	5	MA	MA	MA	MA
Bases de datos	Inadecuada administración de los datos	Fuga de información	5	5	5	15	5	MA	MA	MA	MA
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	1	5	9	3	M	MB	MA	M
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	3	3	4	10	3	M	M	MA	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	4	5	5	14	5	A	MA	MA	MA
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	5	10	3	B	M	MA	M
	No existencia de copias de respaldo	Perdida de información	5	5	5	15	5	MA	MA	MA	MA
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	5	5	5	15	5	MA	MA	MA	MA
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	0	0	5	5	2	D	D	MA	B
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	4	5	5	14	5	MA	MA	MA	MA
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	5	5	15	5	MA	MA	MA	MA
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	0	0	5	5	2	D	D	MA	B

	No existencia de copias de respaldo	Perdida de información	5	5	5	15	5	MA	MA	MA	MA
Balances	Inadecuada administración de los datos	Fuga de información	3	5	5	13	4	M	MA	MA	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	4	5	13	4	M	MA	MA	A
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	5	5	15	5	MA	MA	MA	MA
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	5	5	15	5	MA	MA	MA	MA
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	0	0	5	5	2	D	D	MA	B
	No existencia de copias de respaldo	Perdida de información	5	5	5	15	5	MA	MA	MA	MA
Planillas de pago	Falta de protecciones contra incendios	Incendio	4	5	5	14	5	A	MA	MA	MA
	Falta de instalaciones correctas	Daños por agua	5	5	5	15	5	MA	MA	MA	MA
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	5	5	5	15	5	MA	MA	MA	MA
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	4	5	5	14	5	A	MA	MA	MA
Planillas de servicios	Falta de protecciones contra incendios	Incendio	4	4	5	13	4	A	A	MA	A
	Falta de instalaciones correctas	Daños por agua	5	5	5	15	5	MA	MA	MA	MA
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	3	4	5	12	4	M	A	MA	A

	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	5	5	15	5	MA	MA	MA	MA
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	3	4	5	12	4	M	A	MA	A
	Falta de instalaciones correctas	Daños por agua	4	4	5	13	4	A	A	MA	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	3	4	5	12	4	M	A	MA	A
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	5	5	15	5	MA	MA	MA	MA
Información de los servicios	Falta de protecciones contra incendios	Incendio	4	3	5	13	4	A	A	MA	A
	Falta de instalaciones correctas	Daños por agua	4	4	5	13	4	A	A	MA	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	3	4	5	12	4	M	A	MA	A
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	5	5	15	5	MA	MA	MA	MA
Diagramas de red	Falta de protecciones contra incendios	Incendio	5	5	5	15	5	MA	MA	MA	MA
	Falta de instalaciones correctas	Daños por agua	5	5	5	15	5	MA	MA	MA	MA
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	3	4	4	11	4	M	A	A	A
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	5	5	15	5	MA	MA	MA	MA

Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	5	5	14	5	A	MA	MA	MA
	Ausencia de protecciones digitales	Perdida de equipos	3	3	5	11	4	M	M	MA	A
	Ubicación en área susceptible a desastres	Desastres naturales	3	3	3	9	3	M	M	M	M
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	1	5	8	3	B	MB	MA	M
	Perdida de información	Destrucción de los equipos	5	5	5	15	5	MA	MA	MA	MA
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	0	0	5	5	2	D	D	MA	B
	Ausencia de protecciones digitales	Perdida de equipos	5	3	5	13	4	MA	M	MA	A
	Ubicación en área susceptible a desastres	Desastres naturales	3	3	5	11	4	M	M	MA	A
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	0	0	5	5	2	D	D	MA	B
	Perdida de información	Destrucción de los equipos	5	5	5	15	5	MA	MA	MA	MA
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	1	0	5	6	2	MB	D	MA	B
	Ausencia de protecciones digitales	Perdida de equipos	0	3	5	8	3	D	M	MA	M
	Ubicación en área susceptible a desastres	Desastres naturales	3	3	5	11	4	M	M	MA	A
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	0	0	5	5	2	D	D	MA	B
	Perdida de información	Destrucción de los equipos	5	5	5	15	5	MA	MA	MA	MA
Correo	Interfaz de usuarios complejas	Error en el uso	4	5	5	14	5	A	MA	MA	MA
	Gestión deficiente de contraseñas	Vulneración de la sesión	5	5	5	15	5	MA	MA	MA	MA
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	3	4	5	12	4	M	A	MA	A
	Líneas de comunicación sin protección	Filtración de información	2	5	5	12	4	B	MA	MA	A

	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	1	5	3	9	3	MB	MA	M	M
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	2	2	5	9	3	B	B	MA	M
	No se posee sistema de refrigeración actual	Fallos en los equipos	0	0	5	5	2	D	D	MA	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	5	5	13	4	M	MA	MA	A
	Monitoreo inadecuado de las instalaciones	Robo	5	5	5	15	5	MA	MA	MA	MA
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	0	5	6	2	MB	D	MA	B
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	0	0	5	5	2	D	D	MA	B
	No se posee sistema de refrigeración actual	Fallos en los equipos	0	0	5	5	2	D	D	MA	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	0	0	5	5	2	D	D	MA	B
	Monitoreo inadecuado de las instalaciones	Robo	0	0	5	5	2	D	D	MA	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	0	1	5	6	2	D	MB	MA	B
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	0	0	5	5	2	D	D	MA	B
	No se posee sistema de refrigeración actual	Fallos en los equipos	0	1	5	6	2	D	MB	MA	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	0	0	5	5	2	D	D	MA	B
	Monitoreo inadecuado de las instalaciones	Robo	0	1	5	5	2	D	MB	MA	B

	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	0	0	5	5	2	D	D	MA	B
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	0	0	5	5	2	D	D	MA	B
	No se posee sistema de refrigeración actual	Fallos en los equipos	0	1	5	6	2	D	MB	MA	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	0	0	5	5	2	D	D	MA	B
	Monitoreo inadecuado de las instalaciones	Robo	0	1	5	5	2	D	MB	MA	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	0	0	5	5	2	D	D	MA	B

Anexo 9. Matriz de probabilidad de ocurrencia CID

Nombre del Activo	Vulnerabilidades	Amenazas	Valoración		Valoración total de la probabilidad	Probabilidad de ocurrencia	Magnitud		Magnitud total de la probabilidad
			Degradación	Probabilidad			Degradación	Probabilidad	
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M

	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB

	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M

	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	5	3	B	M	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	5	3	M	B	M
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	1	1	2	1	MB	MB	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	6	3	M	M	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	2	B	B	B
	Falta de conexiones seguras	Error en la manipulación de las redes	2	2	4	2	B	B	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	5	3	B	M	M
S.O Windows	Errores en la configuración de seguridad	Ciberataques	3	3	6	3	M	M	M

	Asignación errada en los accesos	Abuso de los equipos	1	3	4	2	MB	M	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	8	4	A	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	6	3	M	M	M
	Interfaces de difícil manipulación	Errores de uso	2	3	5	3	B	M	M
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	8	4	A	A	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	8	4	A	A	A
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	8	4	A	A	A
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	3	3	6	3	M	M	M
	Asignación errada en los accesos		1	3	4	2	MB	M	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	8	4	A	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	6	3	M	M	M
	Interfaces de difícil manipulación	Errores de uso	2	3	5	3	B	M	M
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	8	4	A	A	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	8	4	A	A	A
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	8	4	A	A	A
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	3	3	6	3	M	M	M
	Asignación errada en los accesos	Abuso de los equipos	1	3	4	2	MB	M	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	8	4	A	A	A

	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	6	3	M	M	M
	Interfaces de difícil manipulación	Errores de uso	2	3	5	3	B	M	M
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	8	4	A	A	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	8	4	A	A	A
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	8	4	A	A	A
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	3	3	6	3	M	M	M
	Asignación errada en los accesos	Abuso de los equipos	1	3	4	2	MB	M	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	8	4	A	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	6	3	M	M	M
	Interfaces de difícil manipulación	Errores de uso	2	3	5	3	B	M	M
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	8	4	A	A	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	8	4	A	A	A
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	8	4	A	A	A
Office 2010	Errores en la configuración de seguridad	Ciberataques	3	3	6	3	M	M	M
	Asignación errada en los accesos	Abuso de los equipos	1	3	4	2	MB	M	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	8	4	A	A	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	3	3	6	3	M	M	M

	Interfaces de difícil manipulación	Errores de uso	2	3	5	3	B	M	M
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	8	4	A	A	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	4	4	8	4	A	A	A
	No existencia de copias de seguridad	Mal funcionamiento del software	4	4	8	4	A	A	A
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	3	2	5	3	M	B	M
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	4	3	7	4	A	M	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	4	4	8	4	A	A	A
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	3	7	4	A	M	M
	No existencia de políticas de mensajería	Perdida de los datos	5	4	9	5	MA	A	MA
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	4	9	5	MA	A	MA
Personal de planta (técnicos, secretarias, contadores, gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	3	2	5	3	M	B	M
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	4	3	7	4	A	M	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	4	4	8	4	A	A	A
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	3	7	4	A	M	M
	No existencia de políticas de mensajería	Perdida de los datos	5	4	9	5	MA	A	MA
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	4	9	5	MA	A	MA

Bases de datos	Inadecuada administración de los datos	Fuga de información	4	4	8	4	A	A	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	6	3	M	M	M
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	2	2	4	2	B	B	B
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	3	2	5	3	M	B	M
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	6	3	M	M	M
	No existencia de copias de respaldo	Perdida de información	4	4	8	4	A	A	A
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	4	4	8	4	A	A	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	6	3	M	M	M
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	2	2	4	2	B	B	B
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	3	2	5	3	M	B	M
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	6	3	M	M	M
	No existencia de copias de respaldo	Perdida de información	4	4	8	4	A	A	A
Balances	Inadecuada administración de los datos	Fuga de información	4	4	8	4	A	A	A

	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	6	3	M	M	M
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	2	2	4	2	B	B	B
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	3	2	5	3	M	B	M
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	6	3	M	M	M
	No existencia de copias de respaldo	Perdida de información	4	4	8	4	A	A	A
Planillas de pago	Falta de protecciones contra incendios	Incendio	2	4	6	3	B	A	M
	Falta de instalaciones correctas	Daños por agua	2	3	5	3	B	M	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	5	3	MB	A	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	6	3	M	M	M
Planillas de servicios	Falta de protecciones contra incendios	Incendio	2	4	6	3	B	A	M
	Falta de instalaciones correctas	Daños por agua	2	3	5	3	B	M	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	5	3	MB	A	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	6	3	M	M	M
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	2	4	6	3	B	A	M
	Falta de instalaciones correctas	Daños por agua	2	3	5	3	B	M	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	5	3	MB	A	M

	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	6	3	M	M	M
Información de los servicios	Falta de protecciones contra incendios	Incendio	2	4	6	3	B	A	M
	Falta de instalaciones correctas	Daños por agua	2	3	5	3	B	M	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	5	3	MB	A	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	6	3	M	M	M
Diagramas de red	Falta de protecciones contra incendios	Incendio	2	4	6	3	B	A	M
	Falta de instalaciones correctas	Daños por agua	2	4	6	3	B	A	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	1	4	5	3	MB	A	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	3	3	6	3	M	M	M
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	4	8	4	A	A	A
	Ausencia de protecciones digitales	Perdida de equipos	0	3	3	2	D	M	M
	Ubicación en área susceptible a desastres	Desastres naturales	2	2	4	2	B	B	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	5	3	M	B	M
	Perdida de información	Destrucción de los equipos	2	2	4	2	B	B	B
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	4	8	4	A	A	A
	Ausencia de protecciones digitales	Perdida de equipos	0	3	3	2	D	M	M
	Ubicación en área susceptible a desastres	Desastres naturales	2	2	4	2	B	B	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	5	3	M	B	M

	Perdida de información	Destrucción de los equipos	2	2	4	2	B	B	B
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	4	4	8	4	A	A	A
	Ausencia de protecciones digitales	Perdida de equipos	0	3	3	2	D	M	M
	Ubicación en área susceptible a desastres	Desastres naturales	2	2	4	2	B	B	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	5	3	M	B	M
	Perdida de información	Destrucción de los equipos	2	2	4	2	B	B	B
Correo	Interfaz de usuarios complejas	Error en el uso	0	1	1	1	D	MB	M
	Gestión deficiente de contraseñas	Vulneración de la sesión	2	3	5	3	B	M	M
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	3	7	4	A	M	M
	Líneas de comunicación sin protección	Filtración de información	1	1	2	1	MB	MB	MB
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	1	1	2	1	MB	MB	MB
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	2	1	MB	MB	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	2	B	B	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	6	3	M	M	M
	Monitoreo inadecuado de las instalaciones	Robo	3	3	6	3	M	M	M
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	2	1	MB	MB	MB
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	2	1	MB	MB	MB

	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	2	B	B	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	6	3	M	M	M
	Monitoreo inadecuado de las instalaciones	Robo	3	3	6	3	M	M	M
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	2	1	MB	MB	MB
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	2	1	MB	MB	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	2	B	B	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	6	3	M	M	M
	Monitoreo inadecuado de las instalaciones	Robo	3	3	6	3	M	M	M
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	2	1	MB	MB	MB
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	1	1	2	1	MB	MB	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	2	B	B	B
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	3	3	6	3	M	M	M
	Monitoreo inadecuado de las instalaciones	Robo	3	3	6	3	M	M	M
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	1	1	2	1	MB	MB	MB

Anexo 10. Matriz de valoración del riesgo

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Magnitud del impacto	Valor de la probabilidad de ocurrencia	Magnitud de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	3	M	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	A	1	MB	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	B	3	M	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	B	2	B	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	A	2	B	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	3	M	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	MA	1	MB	5	B

	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	B	3	M	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	B	2	B	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	A	2	B	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	3	M	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	MA	1	MB	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	1	MB	3	M	3	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	MB	2	B	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	A	2	B	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	4	A	3	M	12	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	B	3	M	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	M	1	MB	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	A	3	M	12	M

	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	M	2	B	6	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	MA	2	B	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	4	A	3	M	12	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	B	3	M	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	M	1	MB	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	A	3	M	12	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	M	2	B	6	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	MA	2	B	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	3	M	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	MA	1	MB	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	M	3	M	9	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	A	2	B	8	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	MA	2	B	10	M

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	3	M	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	B	3	M	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	M	1	MB	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	A	3	M	12	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	A	2	B	8	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	MA	2	B	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	B	3	M	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	A	1	MB	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	M	3	M	9	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	MA	2	B	10	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	MA	2	B	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
	Falta de mantenimiento en el sistema antiincendios	Incendio	4	A	3	M	12	M

Switch de CORE	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	M	3	M	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	MA	1	MB	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	5	MA	3	M	15	A
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	MA	2	B	10	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	MA	2	B	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	B	3	M	6	B
S.O Windows	Errores en la configuración de seguridad	Ciberataques	5	MA	3	M	15	A
	Asignación errada en los accesos	Abuso de los equipos	4	A	2	B	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	A	4	A	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	A	3	M	12	M
	Interfaces de difícil manipulación	Errores de uso	2	B	3	M	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	A	4	A	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	MA	4	A	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	B	4	A	8	B
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	5	MA	3	M	15	A
	Asignación errada en los accesos		4	A	2	B	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	A	4	A	16	A

	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	A	3	M	12	M
	Interfaces de difícil manipulación	Errores de uso	2	B	3	M	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	3	M	4	A	12	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	MA	4	A	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	B	4	A	8	B
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	5	MA	3	M	15	A
	Asignación errada en los accesos	Abuso de los equipos	4	A	2	B	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	A	4	A	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	A	3	M	12	M
	Interfaces de difícil manipulación	Errores de uso	2	B	3	M	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	A	4	A	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	MA	4	A	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	B	4	A	8	B
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	5	MA	3	M	15	A
	Asignación errada en los accesos	Abuso de los equipos	4	A	2	B	8	B
	Ausencia de documentación de uso	Modificación sin autorización	5	MA	4	A	20	MA
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	A	3	M	12	M

	Interfaces de difícil manipulación	Errores de uso	2	B	3	M	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	A	4	A	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	MA	4	A	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	B	4	A	8	B
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	D	3	M	0	MB
	Asignación errada en los accesos	Abuso de los equipos	0	D	2	B	0	MB
	Ausencia de documentación de uso	Modificación sin autorización	4	A	4	A	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	A	3	M	12	M
	Interfaces de difícil manipulación	Errores de uso	2	B	3	M	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	A	4	A	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	MA	4	A	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	B	4	A	8	B
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	MA	3	M	15	A
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	M	4	A	12	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	MA	4	A	20	MA
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	A	4	A	16	A
	No existencia de políticas de mensajería	Perdida de los datos	2	B	5	MA	10	M

	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	MA	5	MA	25	MA
Personal de planta (técnicos, secretarias, contadores, gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	MA	3	M	15	A
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	M	4	A	12	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	MA	4	A	20	MA
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	A	4	A	16	A
	No existencia de políticas de mensajería	Perdida de los datos	4	A	5	MA	20	MA
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	MA	5	MA	25	MA
Bases de datos	Inadecuada administración de los datos	Fuga de información	5	MA	4	A	20	MA
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	M	3	M	9	B
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	3	M	2	B	6	B
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	MA	3	M	15	A
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	M	3	M	9	B
	No existencia de copias de respaldo	Perdida de información	5	MA	4	A	20	MA
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	5	MA	4	A	20	MA
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	2	B	3	M	6	B

	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	MA	2	B	10	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	MA	3	M	15	A
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	B	3	M	6	B
	No existencia de copias de respaldo	Perdida de información	5	MA	4	A	20	MA
Balances	Inadecuada administración de los datos	Fuga de información	4	A	4	A	16	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	A	3	M	12	M
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	MA	2	B	10	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	MA	3	M	15	A
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	B	3	M	6	B
	No existencia de copias de respaldo	Perdida de información	5	MA	4	A	20	MA
Planillas de pago	Falta de protecciones contra incendios	Incendio	5	MA	3	M	15	A
	Falta de instalaciones correctas	Daños por agua	5	MA	3	M	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	5	MA	3	M	15	A
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	MA	3	M	15	A

Planillas de servicios	Falta de protecciones contra incendios	Incendio	4	A	3	M	12	M
	Falta de instalaciones correctas	Daños por agua	5	MA	3	M	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	A	3	M	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	MA	3	M	15	A
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	4	A	3	M	12	M
	Falta de instalaciones correctas	Daños por agua	4	A	3	M	12	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	A	3	M	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	MA	3	M	15	A
Información de los servicios	Falta de protecciones contra incendios	Incendio	4	A	3	M	12	M
	Falta de instalaciones correctas	Daños por agua	4	A	3	M	12	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	A	3	M	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	MA	3	M	15	A
Diagramas de red	Falta de protecciones contra incendios	Incendio	5	MA	3	M	15	A
	Falta de instalaciones correctas	Daños por agua	5	MA	3	M	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	A	3	M	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	MA	3	M	15	A
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	5	MA	4	A	20	MA
	Ausencia de protecciones digitales	Perdida de equipos	4	A	2	B	8	B

	Ubicación en área susceptible a desastres	Desastres naturales	3	M	2	B	6	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	M	3	M	9	B
	Perdida de información	Destrucción de los equipos	5	MA	2	B	10	M
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	B	4	A	8	B
	Ausencia de protecciones digitales	Perdida de equipos	4	A	2	B	8	B
	Ubicación en área susceptible a desastres	Desastres naturales	4	A	2	B	8	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	B	3	M	6	B
	Perdida de información	Destrucción de los equipos	5	MA	2	B	10	M
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	B	4	A	8	B
	Ausencia de protecciones digitales	Perdida de equipos	3	M	2	B	6	B
	Ubicación en área susceptible a desastres	Desastres naturales	4	A	2	B	8	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	B	3	M	6	B
	Perdida de información	Destrucción de los equipos	5	MA	2	B	10	M
Correo	Interfaz de usuarios complejas	Error en el uso	5	MA	1	MB	5	B
	Gestión deficiente de contraseñas	Vulneración de la sesión	5	MA	3	M	15	A
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	A	4	A	16	A
	Líneas de comunicación sin protección	Filtración de información	4	A	1	MB	4	MB
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	3	M	1	MB	3	MB
	Falta de mantenimiento en el sistema antiincendios	Incendio	3	M	1	MB	3	MB

Control de acceso								
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	B	2	B	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	A	3	M	12	M
	Monitoreo inadecuado de las instalaciones	Robo	5	MA	3	M	15	A
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	B	1	MB	2	MB
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	2	B	1	MB	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	B	2	B	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	B	3	M	6	B
	Monitoreo inadecuado de las instalaciones	Robo	2	B	3	M	6	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	B	1	MB	2	MB
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	2	B	1	MB	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	B	2	B	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	B	3	M	6	B
	Monitoreo inadecuado de las instalaciones	Robo	2	B	3	M	6	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	B	1	MB	2	MB
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	2	B	1	MB	2	MB

	No se posee sistema de refrigeración actual	Fallos en los equipos	2	B	2	B	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	B	3	M	6	B
	Monitoreo inadecuado de las instalaciones	Robo	2	B	3	M	6	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	B	1	MB	2	MB

Anexo 11. Matriz de calor

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B

Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	1	3	3	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M

	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	6	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	6	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	9	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	8	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
Router	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B

MIKROTIK	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	8	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	9	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	10	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	5	3	15	A
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	10	M

	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B
S.O Windows	Errores en la configuración de seguridad	Ciberataques	5	3	15	A
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	5	3	15	A
	Asignación errada en los accesos		4	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	3	4	12	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B
	Errores en la configuración de seguridad	Ciberataques	5	3	15	A

Software de administración de red U2000	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	5	3	15	A
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	5	4	20	MA
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	3	0	MB
	Asignación errada en los accesos	Abuso de los equipos	0	2	0	MB
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M

	Interfaces de difícil manipulación	Errores de uso	2	3	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	15	A
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	12	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	20	MA
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	4	16	A
	No existencia de políticas de mensajería	Perdida de los datos	2	5	10	M
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	25	MA
Personal de planta (técnicos, secretarias, contadores, gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	15	A
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	12	M
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	20	MA
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	4	16	A
	No existencia de políticas de mensajería	Perdida de los datos	4	5	20	MA
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	25	MA
Bases de datos	Inadecuada administración de los datos	Fuga de información	5	4	20	MA
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	9	B

	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	3	2	6	B
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	9	B
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	5	4	20	MA
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	2	3	6	B
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	10	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	6	B
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA
Balances	Inadecuada administración de los datos	Fuga de información	4	4	16	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	3	12	M
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	10	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	6	B

	No existencia de copias de respaldo	Perdida de información	5	4	20	MA
Planillas de pago	Falta de protecciones contra incendios	Incendio	5	3	15	A
	Falta de instalaciones correctas	Daños por agua	5	3	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	5	3	15	A
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A
Planillas de servicios	Falta de protecciones contra incendios	Incendio	4	3	12	M
	Falta de instalaciones correctas	Daños por agua	5	3	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	4	3	12	M
	Falta de instalaciones correctas	Daños por agua	4	3	12	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A
Información de los servicios	Falta de protecciones contra incendios	Incendio	4	3	12	M
	Falta de instalaciones correctas	Daños por agua	4	3	12	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A
	Falta de protecciones contra incendios	Incendio	5	3	15	A

Diagramas de red	Falta de instalaciones correctas	Daños por agua	5	3	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	5	4	20	MA
	Ausencia de protecciones digitales	Perdida de equipos	4	2	8	B
	Ubicación en área susceptible a desastres	Desastres naturales	3	2	6	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	3	9	B
	Perdida de información	Destrucción de los equipos	5	2	10	M
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	4	8	B
	Ausencia de protecciones digitales	Perdida de equipos	4	2	8	B
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	8	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	3	6	B
	Perdida de información	Destrucción de los equipos	5	2	10	M
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	4	8	B
	Ausencia de protecciones digitales	Perdida de equipos	3	2	6	B
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	8	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	3	6	B
	Perdida de información	Destrucción de los equipos	5	2	10	M
Correo	Interfaz de usuarios complejas	Error en el uso	5	1	5	B

	Gestión deficiente de contraseñas	Vulneración de la sesión	5	3	15	A
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	4	16	A
	Líneas de comunicación sin protección	Filtración de información	4	1	4	MB
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	3	1	3	MB
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	3	1	3	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	3	12	M
	Monitoreo inadecuado de las instalaciones	Robo	5	3	15	A
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B

	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB

Anexo 12. Salvaguardas

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo	Controles existentes
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB	Control interno departamento de tecnología

	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	1	3	3	MB	No aplica

	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	6	B	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	6	B	No aplica

	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	9	B	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	8	B	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	8	B	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	6	B	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	9	B	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	10	M	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M	Extintores, Alarmas de humo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	5	3	15	A	No aplica
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	10	M	No aplica
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo
S.O Windows	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico Acceso solo al personal autorizado
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B	Acceso personal autorizado Controles de acceso físico
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Capacitación y documentación de uso
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico Acceso solo al personal autorizado
	Asignación errada en los accesos		4	2	8	B	Acceso personal autorizado Controles de acceso físico
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica

	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Capacitación y documentación de uso
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	3	4	12	M	Capacitación online
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico Acceso solo al personal autorizado
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B	Acceso personal autorizado Controles de acceso físico
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	No aplica
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B	Acceso personal autorizado

	Ausencia de documentación de uso	Modificación sin autorización	5	4	20	MA	No aplica
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Capacitación online
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	3	0	MB	Controles de acceso físico
	Asignación errada en los accesos	Abuso de los equipos	0	2	0	MB	Acceso personal autorizado
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Documentos del sitio oficial
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	15	A	Capacitación
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	12	M	No aplica
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	20	MA	Ordenes de trabajo

	Entrenamiento insuficiente del personal	Perdida de personal clave	4	4	16	A	Capacitación online
	No existencia de políticas de mensajería	Perdida de los datos	2	5	10	M	Capacitación online
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	25	MA	No aplica
Personal de planta (técnicos, secretarias, contadores , gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	15	A	Capacitación
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	12	M	No aplica
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	20	MA	Ordenes de trabajo
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	4	16	A	Capacitación online y presencial
	No existencia de políticas de mensajería	Perdida de los datos	4	5	20	MA	Capacitación presencial
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	25	MA	No aplica
Bases de datos	Inadecuada administración de los datos	Fuga de información	5	4	20	MA	Proveedor externo
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	9	B	Extintores, Alarmas de humo
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	3	2	6	B	Capacitación
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A	No aplica
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	9	B	Mecanismos de climatización
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA	Mecanismos físicos de respaldo
	Inadecuada administración de los datos	Fuga de información	5	4	20	MA	Proveedor externo

Documentos compartidos	Falta de protecciones físicas adecuadas	Daños por agua o fuego	2	3	6	B	Extintores, Alarmas de humo
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	10	M	Capacitación
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A	No aplica
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	6	B	Mecanismos de climatización
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA	Mecanismos físicos de respaldo
Balances	Inadecuada administración de los datos	Fuga de información	4	4	16	A	Proveedor externo
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	3	12	M	Extintores, Alarmas de humo
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	10	M	Capacitación
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A	No aplica
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	6	B	Mecanismos de climatización
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA	Mecanismos físicos de respaldo
Planillas de pago	Falta de protecciones contra incendios	Incendio	5	3	15	A	Alarmas de humo, Extintores
	Falta de instalaciones correctas	Daños por agua	5	3	15	A	Controles internos
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	5	3	15	A	Mecanismos de climatización

	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica
Planillas de servicios	Falta de protecciones contra incendios	Incendio	4	3	12	M	Alarmas de humo, Extintores
	Falta de instalaciones correctas	Daños por agua	5	3	15	A	Controles internos
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	4	3	12	M	Alarmas de humo, Extintores
	Falta de instalaciones correctas	Daños por agua	4	3	12	M	Controles internos
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica
Información de los servicios	Falta de protecciones contra incendios	Incendio	4	3	12	M	Alarmas de humo, Extintores
	Falta de instalaciones correctas	Daños por agua	4	3	12	M	Controles internos
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica
	Falta de protecciones contra incendios	Incendio	5	3	15	A	Alarmas de humo,

Diagramas de red							Extintores
	Falta de instalaciones correctas	Daños por agua	5	3	15	A	Controles internos
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	5	4	20	MA	Acceso personal autorizado
	Ausencia de protecciones digitales	Perdida de equipos	4	2	8	B	Controles físicos
	Ubicación en área susceptible a desastres	Desastres naturales	3	2	6	B	Mecanismos de climatización
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	3	9	B	Utilización de UPS
	Perdida de información	Destrucción de los equipos	5	2	10	M	Capacitación sobre el uso de los equipos
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	4	8	B	Acceso personal autorizado
	Ausencia de protecciones digitales	Perdida de equipos	4	2	8	B	Controles físicos
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	8	B	Mecanismos de climatización
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	3	6	B	No aplica
	Perdida de información	Destrucción de los equipos	5	2	10	M	No aplica
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	4	8	B	Acceso personal autorizado

	Ausencia de protecciones digitales	Perdida de equipos	3	2	6	B	Controles físicos
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	8	B	Mecanismos de climatización
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	3	6	B	Utilización de UPS
	Perdida de información	Destrucción de los equipos	5	2	10	M	Capacitación sobre el uso de los equipos
Correo	Interfaz de usuarios complejas	Error en el uso	5	1	5	B	Documentación del sitio oficial
	Gestión deficiente de contraseñas	Vulneración de la sesión	5	3	15	A	Capacitación online
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	4	16	A	Acceso personal autorizado, Capacitación
	Líneas de comunicación sin protección	Filtración de información	4	1	4	MB	No aplica
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	3	1	3	MB	No aplica
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	3	1	3	MB	Extintores, Alarmas de humo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización,
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	3	12	M	Capacitación física
	Monitoreo inadecuado de las instalaciones	Robo	5	3	15	A	No aplica
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza

UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB	Extintores, Alarmas de humo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización,
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B	Capacitación física
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B	No aplica
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB	Extintores, Alarmas de humo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización,
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B	Capacitación física
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B	No aplica
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB	Extintores, Alarmas de humo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización,
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B	Capacitación física
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B	No aplica

	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza

Anexo 13. Opción de tratamiento de riesgos

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad de ocurrencia	Valor del riesgo	Magnitud del riesgo	Controles existentes	Opciones de tratamiento del riesgo
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B	No aplica	Aceptar riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes	Aceptar riesgo

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	3	6	B	No aplica	Aceptar riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes	Aceptar riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología	Aceptar riesgo

	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	1	3	3	MB	No aplica	Aceptar riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	4	MB	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	8	B	Gestión de redes	Aceptar riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M	Extintores, Alarmas de humo	Reducir riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M	No aplica	Reducir riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	6	B	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes	Reducir riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M	Extintores, Alarmas de humo	Reducir riesgo

	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M	No aplica	Reducir riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	6	B	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes	Reducir riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	9	B	No aplica	Aceptar riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	8	B	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes	Reducir riesgo

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	3	6	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	3	MB	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	3	12	M	No aplica	Reducir riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	8	B	No aplica	Aceptar riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes	Reducir riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	3	6	B	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	4	MB	Control interno departamento de tecnología	Aceptar riesgo

	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	3	9	B	No aplica	Aceptar riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	10	M	No aplica	Reducir riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes	Reducir riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	4	3	12	M	Extintores, Alarmas de humo	Reducir riesgo
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	3	9	B	Plan de mantenimiento preventivo	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	5	B	Control interno departamento de tecnología	Aceptar riesgo
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	10	M	No aplica	Reducir riesgo
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	10	M	Gestión de redes	Reducir riesgo
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	3	6	B	Configuración proveedor externo	Aceptar riesgo
S.O Windows	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Trasferir el riesgo

	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B	Acceso personal autorizado Controles de acceso físico	Aceptar riesgo
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica	Reducir o Trasferir el riesgo
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online	Reducir riesgo
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Capacitación y documentación de uso	Aceptar riesgo
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online	Reducir o Trasferir el riesgo
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica	Aceptar riesgo
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Trasferir el riesgo
	Asignación errada en los accesos		4	2	8	B	Acceso personal autorizado Controles de acceso físico	Aceptar riesgo
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica	Reducir o Trasferir el riesgo

	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online	Reducir riesgo
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Capacitación y documentación de uso	Aceptar riesgo
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	3	4	12	M	Capacitación online	Reducir riesgo
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica	Aceptar riesgo
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Trasferir el riesgo
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B	Acceso personal autorizado Controles de acceso físico	Aceptar riesgo
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica	Reducir o Trasferir el riesgo
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online	Reducir riesgo
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	No aplica	Aceptar riesgo
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online	Reducir o Trasferir el riesgo
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online	Reducir, Transferir o

								Evitar el riesgo
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica	Aceptar riesgo
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	5	3	15	A	Controles de acceso físico	Reducir o Trasferir el riesgo
	Asignación errada en los accesos	Abuso de los equipos	4	2	8	B	Acceso personal autorizado	Aceptar riesgo
	Ausencia de documentación de uso	Modificación sin autorización	5	4	20	MA	No aplica	Reducir, Transferir o Evitar el riesgo
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online	Reducir riesgo
	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Capacitación online	Aceptar riesgo
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online	Reducir o Trasferir el riesgo
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica	Aceptar riesgo
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	3	0	MB	Controles de acceso físico	Aceptar riesgo
	Asignación errada en los accesos	Abuso de los equipos	0	2	0	MB	Acceso personal autorizado	Aceptar riesgo
	Ausencia de documentación de uso	Modificación sin autorización	4	4	16	A	No aplica	Reducir o Trasferir el riesgo
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	3	12	M	Capacitación online	Reducir riesgo

	Interfaces de difícil manipulación	Errores de uso	2	3	6	B	Documentos del sitio oficial	Aceptar riesgo
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	4	16	A	Capacitación online	Reducir o Trasferir el riesgo
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	4	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo
	No existencia de copias de seguridad	Mal funcionamiento del software	2	4	8	B	No aplica	Aceptar riesgo
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	15	A	Capacitación	Reducir o Trasferir el riesgo
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	12	M	No aplica	Reducir riesgo
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	20	MA	Ordenes de trabajo	Reducir, Transferir o Evitar el riesgo
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	4	16	A	Capacitación online	Reducir o Trasferir el riesgo
	No existencia de políticas de mensajería	Perdida de los datos	2	5	10	M	Capacitación online	Reducir riesgo
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	25	MA	No aplica	Reducir, Transferir o Evitar el riesgo
Personal de planta	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	15	A	Capacitación	Reducir o Trasferir el riesgo

(técnicos, secretarias, contadores , gerencia)	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	4	12	M	No aplica	Reducir riesgo
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	4	20	MA	Ordenes de trabajo	Reducir, Transferir o Evitar el riesgo
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	4	16	A	Capacitación online y presencial	Reducir o Trasferir el riesgo
	No existencia de políticas de mensajería	Perdida de los datos	4	5	20	MA	Capacitación presencial	Reducir, Transferir o Evitar el riesgo
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	5	25	MA	No aplica	Reducir, Transferir o Evitar el riesgo
Bases de datos	Inadecuada administración de los datos	Fuga de información	5	4	20	MA	Proveedor externo	Reducir, Transferir o Evitar el riesgo
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	3	9	B	Extintores, Alarmas de humo	Aceptar riesgo
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	3	2	6	B	Capacitación	Aceptar riesgo
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	3	9	B	Mecanismos de climatización	Aceptar riesgo

	No existencia de copias de respaldo	Perdida de información	5	4	20	MA	Mecanismos físicos de respaldo	Reducir, Transferir o Evitar el riesgo
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	5	4	20	MA	Proveedor externo	Reducir, Transferir o Evitar el riesgo
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	2	3	6	B	Extintores, Alarmas de humo	Aceptar riesgo
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	10	M	Capacitación	Reducir riesgo
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	6	B	Mecanismos de climatización	Aceptar riesgo
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA	Mecanismos físicos de respaldo	Reducir, Transferir o Evitar el riesgo
Balances	Inadecuada administración de los datos	Fuga de información	4	4	16	A	Proveedor externo	Reducir o Trasferir el riesgo
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	3	12	M	Extintores, Alarmas de humo	Reducir riesgo
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	10	M	Capacitación	Reducir riesgo
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	3	15	A	No aplica	Reducir o Trasferir el riesgo

	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	3	6	B	Mecanismos de climatización	Aceptar riesgo
	No existencia de copias de respaldo	Perdida de información	5	4	20	MA	Mecanismos físicos de respaldo	Reducir, Transferir o Evitar el riesgo
Planillas de pago	Falta de protecciones contra incendios	Incendio	5	3	15	A	Alarmas de humo, Extintores	Reducir o Trasferir el riesgo
	Falta de instalaciones correctas	Daños por agua	5	3	15	A	Controles internos	Reducir o Trasferir el riesgo
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	5	3	15	A	Mecanismos de climatización	Reducir o Trasferir el riesgo
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
Planillas de servicios	Falta de protecciones contra incendios	Incendio	4	3	12	M	Alarmas de humo, Extintores	Reducir riesgo
	Falta de instalaciones correctas	Daños por agua	5	3	15	A	Controles internos	Reducir o Trasferir el riesgo
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización	Reducir riesgo
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	4	3	12	M	Alarmas de humo, Extintores	Reducir riesgo

	Falta de instalaciones correctas	Daños por agua	4	3	12	M	Controles internos	Reducir riesgo
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización	Reducir riesgo
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
Información de los servicios	Falta de protecciones contra incendios	Incendio	4	3	12	M	Alarmas de humo, Extintores	Reducir riesgo
	Falta de instalaciones correctas	Daños por agua	4	3	12	M	Controles internos	Reducir riesgo
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización	Reducir riesgo
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
Diagramas de red	Falta de protecciones contra incendios	Incendio	5	3	15	A	Alarmas de humo, Extintores	Reducir o Trasferir el riesgo
	Falta de instalaciones correctas	Daños por agua	5	3	15	A	Controles internos	Reducir o Trasferir el riesgo
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	3	12	M	Mecanismos de climatización	Reducir riesgo
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	5	4	20	MA	Acceso personal autorizado	Reducir, Transferir o Evitar el riesgo

	Ausencia de protecciones digitales	Perdida de equipos	4	2	8	B	Controles físicos	Aceptar riesgo
	Ubicación en área susceptible a desastres	Desastres naturales	3	2	6	B	Mecanismos de climatización	Aceptar riesgo
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	3	9	B	Utilización de UPS	Aceptar riesgo
	Perdida de información	Destrucción de los equipos	5	2	10	M	Capacitación sobre el uso de los equipos	Reducir riesgo
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	4	8	B	Acceso personal autorizado	Aceptar riesgo
	Ausencia de protecciones digitales	Perdida de equipos	4	2	8	B	Controles físicos	Aceptar riesgo
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	8	B	Mecanismos de climatización	Aceptar riesgo
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	3	6	B	No aplica	Aceptar riesgo
	Perdida de información	Destrucción de los equipos	5	2	10	M	No aplica	Reducir riesgo
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	4	8	B	Acceso personal autorizado	Aceptar riesgo
	Ausencia de protecciones digitales	Perdida de equipos	3	2	6	B	Controles físicos	Aceptar riesgo
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	8	B	Mecanismos de climatización	Aceptar riesgo
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	3	6	B	Utilización de UPS	Aceptar riesgo
	Perdida de información	Destrucción de los equipos	5	2	10	M	Capacitación sobre el uso de los equipos	Reducir riesgo

Correo	Interfaz de usuarios complejas	Error en el uso	5	1	5	B	Documentación del sitio oficial	Aceptar riesgo
	Gestión deficiente de contraseñas	Vulneración de la sesión	5	3	15	A	Capacitación online	Reducir o Trasferir el riesgo
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	4	16	A	Acceso personal autorizado, Capacitación	Reducir o Trasferir el riesgo
	Líneas de comunicación sin protección	Filtración de información	4	1	4	MB	No aplica	Aceptar riesgo
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	3	1	3	MB	No aplica	Aceptar riesgo
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	3	1	3	MB	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización ,	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	3	12	M	Capacitación física	Reducir riesgo
	Monitoreo inadecuado de las instalaciones	Robo	5	3	15	A	No aplica	Reducir o Trasferir el riesgo
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza	Aceptar riesgo
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización ,	Aceptar riesgo

	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B	Capacitación física	Aceptar riesgo
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B	No aplica	Aceptar riesgo
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza	Aceptar riesgo
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización ,	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B	Capacitación física	Aceptar riesgo
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B	No aplica	Aceptar riesgo
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	2	MB	Limpieza diaria por parte del personal de limpieza	Aceptar riesgo
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	2	MB	Extintores, Alarmas de humo	Aceptar riesgo
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	4	MB	Sistema de climatización ,	Aceptar riesgo
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	3	6	B	Capacitación física	Aceptar riesgo
	Monitoreo inadecuado de las instalaciones	Robo	2	3	6	B	No aplica	Aceptar riesgo
	No existe las medidas adecuadas para el	Corrosión	2	1	2	MB	Limpieza diaria por	Aceptar riesgo

	almacenamiento de los equipos						parte del personal de limpieza	

Anexo 14. Acciones correctivas para el tratamiento del riesgo

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del riesgo	Magnitud del riesgo	Controles existentes	Opciones de tratamiento del riesgo	Acciones de tratamiento	Justificación
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	12	M	Extintores, Alarmas de humo	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incendios
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	12	M	No aplica	Reducir riesgo	Restricción de acceso, Incorporar videovigilancia	Las acciones antes mencionadas generan un mejor control en las instalaciones de la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al	No se posee seguridad en la

							ingresar a las redes de la empresa	gestión de las redes
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	12	M	Extintores, Alarmas de humo	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incendios
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	12	M	No aplica	Reducir riesgo	Restricción de acceso, Incorporar videovigilancia	Las acciones antes mencionadas generan un mejor control en las instalaciones de la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al ingresar a las redes de la empresa	No se posee seguridad en la gestión de las redes
FIREWALL	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al ingresar a las redes de la empresa	No se posee seguridad en la gestión de las redes
Router MIKROTIK	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	12	M	No aplica	Reducir riesgo	Restricción de acceso, Incorporar videovigilancia	Las acciones antes mencionadas generan un mejor control en las instalaciones de la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al	No se posee seguridad en la

							ingresar a las redes de la empresa	gestión de las redes
Switch	No existe control sobre las personas que ingresan y salen de la organización	Robo	10	M	No aplica	Reducir riesgo	Restricción de acceso, Incorporar videovigilancia	Las acciones antes mencionadas generan un mejor control en las instalaciones de la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al ingresar a las redes de la empresa	No se posee seguridad en la gestión de las redes
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	12	M	Extintores, Alarmas de humo	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incendios
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	15	A	No aplica	Reducir o Transferir el riesgo	Generar un registro de activos, Restringir el ingreso, Incorporar videovigilancia	No se posee un registro de los activos que posee la empresa
	No existe control sobre las personas que ingresan y salen de la organización	Robo	10	M	No aplica	Reducir riesgo	Restricción de acceso, Incorporar videovigilancia	Las acciones antes mencionadas generan un mejor control en las instalaciones de la empresa

	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	Gestión de redes	Reducir riesgo	Incorporar niveles de seguridad al ingresar a las redes de la empresa	No se posee seguridad en la gestión de las redes
S.O Windows	Errores en la configuración de seguridad	Ciberataques	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Transferir el riesgo	Capacitar al personal, Escaneo de dispositivos Generar redes de invitados para personal externo	En la actualizad en la empresa no se realiza ninguna de las acciones antes mencionadas por lo cual no existe este tipo de control
	Ausencia de documentación de uso	Modificación sin autorización	16	A	No aplica	Reducir o Transferir el riesgo	Generar documentos de usuario	No existe la documentación
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	Capacitación online	Reducir riesgo	Generar documentos de usuario	No existe la documentación
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	16	A	Capacitación online	Reducir o Transferir el riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de contraseñas y su manipulación	No existe capacitación al personal
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Transferir el riesgo	Capacitar al personal, Escaneo de dispositivos Generar redes de invitados para personal externo	En la actualizad en la empresa no se realiza ninguna de las acciones antes mencionadas por lo cual no existe este tipo de control

	Ausencia de documentación de uso	Modificación sin autorización	16	A	No aplica	Reducir o Transferir el riesgo	Generar documentos de usuario	No existe la documentación
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	Capacitación online	Reducir riesgo	Generar documentos de usuario	No existe la documentación
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	12	M	Capacitación online	Reducir riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de contraseñas y su manipulación	No existe capacitación al personal
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	15	A	Controles de acceso físico Acceso solo al personal autorizado	Reducir o Transferir el riesgo	Capacitar al personal, Escaneo de dispositivos Generar redes de invitados para personal externo	En la actualizad en la empresa no se realiza ninguna de las acciones antes mencionadas por lo cual no existe este tipo de control
	Ausencia de documentación de uso	Modificación sin autorización	16	A	No aplica	Reducir o Transferir el riesgo	Generar documentos de usuario	No existe la documentación
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	Capacitación online	Reducir riesgo	Generar documentos de usuario	No existe la documentación
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	16	A	Capacitación online	Reducir o Transferir el riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	20	MA	Capacitación online	Reducir, Transferir	Capacitación sobre la generación de	No existe capacitación al personal

						o Evitar el riesgo	contraseñas y su manipulación	
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	15	A	Controles de acceso físico	Reducir o Transferir el riesgo	Capacitar al personal, Escaneo de dispositivos Generar redes de invitados para personal externo	En la actualizad en la empresa no se realiza ninguna de las acciones antes mencionadas por lo cual no existe este tipo de control
	Ausencia de documentación de uso	Modificación sin autorización	20	MA	No aplica	Reducir, Transferir o Evitar el riesgo	Generar documentos de usuario	No existe la documentación
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	Capacitación online	Reducir riesgo	Generar documentos de usuario	No existe la documentación
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	16	A	Capacitación online	Reducir o Transferir el riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de contraseñas y su manipulación	No existe capacitación al personal
Office 2010	Ausencia de documentación de uso	Modificación sin autorización	16	A	No aplica	Reducir o Transferir el riesgo	Generar documentos de usuario, Restricción de ingreso	No existe la documentación o control de ingreso
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	Capacitación online	Reducir riesgo	Generar guías de mantenimiento de los sistemas	No existe la documentación
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	16	A	Capacitación online	Reducir o Transferir el riesgo	Generación de las políticas de uso de los equipos,	No existe una capacitación al personal sobre

							Capacitación al personal	seguridad de los equipos
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	20	MA	Capacitación online	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de contraseñas y su manipulación	No existe capacitación al personal
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	15	A	Capacitación	Reducir o Transferir el riesgo	Generar la documentación de usuario	No existe documentos que ayuden a la utilización de los equipos
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	12	M	No aplica	Reducir riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	20	MA	Ordenes de trabajo	Reducir, Transferir o Evitar el riesgo	Capacitar a personal sobre el uso correcto de los equipos	
	Entrenamiento insuficiente del personal	Perdida de personal clave	16	A	Capacitación online	Reducir o Transferir el riesgo	Capacitación al personal nuevo	No se realiza la capacitación al nevo personal
	No existencia de políticas de mensajería	Perdida de los datos	10	M	Capacitación online	Reducir riesgo	Utilización de políticas de mensajería, Capacitación	No se posee políticas de seguridad
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	25	MA	No aplica	Reducir, Transferir o Evitar el riesgo	Capacitación al personal	No se posee los conocimientos necesarios
Personal de planta (técnicos, secretarias,	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	15	A	Capacitación	Reducir o Transferir el riesgo	Generar la documentación de usuario	No existe documentos que ayuden a la utilización de los equipos

contadores , gerencia)	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	12	M	No aplica	Reducir riesgo	Generación de las políticas de uso de los equipos, Capacitación al personal	No existe una capacitación al personal sobre seguridad de los equipos
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	20	MA	Ordenes de trabajo	Reducir, Transferir o Evitar el riesgo	Capacitar a personal sobre el uso correcto de los equipos	
	Entrenamiento insuficiente del personal	Perdida de personal clave	16	A	Capacitación online y presencial	Reducir o Transferir el riesgo	Capacitación al personal nuevo	No se realiza la capacitación al nevo personal
	No existencia de políticas de mensajería	Perdida de los datos	20	MA	Capacitación presencial	Reducir, Transferir o Evitar el riesgo	Utilización de políticas de mensajería, Capacitación	No se posee políticas de seguridad
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	25	MA	No aplica	Reducir, Transferir o Evitar el riesgo	Capacitación al personal	No se posee los conocimientos necesarios
Bases de datos	Inadecuada administración de los datos	Fuga de información	20	MA	Proveedor externo	Reducir, Transferir Evitar el riesgo	Incorporación de seguridad, Capacitación	No existen políticas de seguridad ni la capacitación adecuada
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	15	A	No aplica	Reducir o Transferir el riesgo	Generar modelos de contratos según las políticas de seguridad	No existen políticas de seguridad
	No existencia de copias de respaldo	Perdida de información	20	MA	Mecanismos físicos de respaldo	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de respaldos de la información	No se realiza una generación de los respaldos periódica
Documentos	Inadecuada administración de los datos	Fuga de información	20	MA	Proveedor externo	Reducir, Transferir Evitar el riesgo	Incorporación de seguridad, Capacitación	No existen políticas de seguridad ni la capacitación adecuada

compartidos	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	10	M	Capacitación	Reducir riesgo	Capacitación al personal nuevo	No se realiza una capacitación sobre los procesos de la empresa
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	15	A	No aplica	Reducir o Transferir el riesgo	Generar modelos de contratos según las políticas de seguridad	No existen políticas de seguridad
	No existencia de copias de respaldo	Perdida de información	20	MA	Mecanismos físicos de respaldo	Reducir, Transferir o Evitar el riesgo	Capacitación sobre la generación de respaldos de la información	No se realiza una generación de los respaldos periódica
Balances	Inadecuada administración de los datos	Fuga de información	16	A	Proveedor externo	Reducir o Transferir el riesgo	Incorporación de seguridad, Capacitación	No existen políticas de seguridad ni la capacitación adecuada
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	12	M	Extintores, Alarmas de humo	Reducir riesgo	Mejorar los sistemas antiincendios, Incorporar personal	No se posee controles adecuados para el manejo de las amenazas del fuego o el agua
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	10	M	Capacitación	Reducir riesgo	Capacitación al personal nuevo	No se realiza una capacitación sobre los procesos de la empresa
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	15	A	No aplica	Reducir o Transferir el riesgo	Generar modelos de contratos según las políticas de seguridad	No existen políticas de seguridad
	No existencia de copias de respaldo	Perdida de información	20	MA	Mecanismos físicos de respaldo	Reducir, Transferir	Capacitación sobre la generación de	No se realiza una generación

						o Evitar el riesgo	respaldos de la información	de los respaldos periódica
Planillas de pago	Falta de protecciones contra incendios	Incendio	15	A	Alarmas de humo, Extintores	Reducir o Transferir el riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incendios
	Falta de instalaciones correctas	Daños por agua	15	A	Controles internos	Reducir o Transferir el riesgo	Incorporación de personal de seguridad, Restricción del ingreso	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los daños
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	15	A	Mecanismos de climatización	Reducir o Transferir el riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incidentes generados por la naturaleza
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	15	A	No aplica	Reducir o Transferir el riesgo	Generación de políticas sobre el uso de la documentación y capacitación sobre seguridad	No existen políticas de seguridad

Planillas de servicios	Falta de protecciones contra incendios	Incendio	12	M	Alarmas de humo, Extintores	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incendios
	Falta de instalaciones correctas	Daños por agua	15	A	Controles internos	Reducir o Transferir el riesgo	Incorporación de personal de seguridad, Restricción del ingreso	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los daños
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	12	M	Mecanismos de climatización	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incidentes generados por la naturaleza
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	15	A	No aplica	Reducir o Transferir el riesgo	Generación de políticas sobre el uso de la documentación y capacitación sobre seguridad	No existen políticas de seguridad
	Falta de protecciones contra incendios	Incendio	12	M	Alarmas de humo,	Reducir riesgo	Mantenimiento continuo de los	Se debe incorporar

Ordenes de trabajo					Extintores		sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	seguridades extras las cuales ayuden a detectar o mitigar los incendios
	Falta de instalaciones correctas	Daños por agua	12	M	Controles internos	Reducir riesgo	Incorporación de personal de seguridad, Restricción del ingreso	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los daños
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	12	M	Mecanismos de climatización	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incidentes generados por la naturaleza
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	15	A	No aplica	Reducir o Transferir el riesgo	Generación de políticas sobre el uso de la documentación y capacitación sobre seguridad	No existen políticas de seguridad
	Falta de protecciones contra incendios	Incendio	12	M	Alarmas de humo, Extintores	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios,	Se debe incorporar seguridades extras las

Información de los servicios							Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	cuales ayuden a detectar o mitigar los incendios
	Falta de instalaciones correctas	Daños por agua	12	M	Controles internos	Reducir riesgo	Incorporación de personal de seguridad, Restricción del ingreso	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los daños
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	12	M	Mecanismos de climatización	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incidentes generados por la naturaleza
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	15	A	No aplica	Reducir o Transferir el riesgo	Generación de políticas sobre el uso de la documentación y capacitación sobre seguridad	No existen políticas de seguridad
Diagramas de red	Falta de protecciones contra incendios	Incendio	15	A	Alarmas de humo, Extintores	Reducir o Transferir el riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de	Se debe incorporar seguridades extras las cuales ayuden a detectar o

							seguridad, Restricción del ingreso, Climatización del lugar	mitigar los incendios
	Falta de instalaciones correctas	Daños por agua	15	A	Controles internos	Reducir o Transferir el riesgo	Incorporación de personal de seguridad, Restricción del ingreso	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los daños
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	12	M	Mecanismos de climatización	Reducir riesgo	Mantenimiento continuo de los sistemas antiincendios, Incorporación de personal de seguridad, Restricción del ingreso, Climatización del lugar	Se debe incorporar seguridades extras las cuales ayuden a detectar o mitigar los incidentes generados por la naturaleza
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	15	A	No aplica	Reducir o Transferir el riesgo	Generación de políticas sobre el uso de la documentación y capacitación sobre seguridad	No existen políticas de seguridad
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	20	MA	Acceso personal autorizado	Reducir, Transferir o Evitar el riesgo	Control de acceso, Incorporar videovigilancia	No existe controles de monitorización en las áreas
	Perdida de información	Destrucción de los equipos	10	M	Capacitación sobre el uso de los equipos	Reducir riesgo	Capacitación sobre el uso de los equipos que posee la empresa	No existe una capacitación al personal

Vehículos	Perdida de información	Destrucción de los equipos	10	M	No aplica	Reducir riesgo	Capacitación sobre el uso de los equipos que posee la empresa	No existe una capacitación al personal
Antenas	Perdida de información	Destrucción de los equipos	10	M	Capacitación sobre el uso de los equipos	Reducir riesgo	Capacitación sobre el uso de los equipos que posee la empresa	No existe una capacitación al personal
Correo	Gestión deficiente de contraseñas	Vulneración de la sesión	15	A	Capacitación online	Reducir o Transferir el riesgo	Capacitación sobre el uso correcto de las credenciales y ciberseguridad	No se realiza capacitación al personal sobre el uso correcto de las credenciales
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	16	A	Acceso personal autorizado, Capacitación	Reducir o Transferir el riesgo	Capacitación sobre el uso adecuado de los equipos al momento de dejar el puesto de trabajo	No se emplea niveles de seguridad al dejar el puesto de trabajo
Control de acceso	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	12	M	Capacitación física	Reducir riesgo	Capacitación sobre el uso de los equipos	No se realiza capacitación al personal
	Monitoreo inadecuado de las instalaciones	Robo	15	A	No aplica	Reducir o Transferir el riesgo	Control de acceso, Incorporar videovigilancia	No existe controles de monitorización en las áreas

Anexo 15. Cálculo del riesgo residual

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del Impacto CID	Valor de la probabilidad residual			Valor del riesgo residual	Magnitud del riesgo
				Degradación	Probabilidad	Total		
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	3	2	2	2	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	1	1	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	2	2	2	4	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	2	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
Pcs Escritorio	Falta de mantenimiento en el sistema antiincendios	Incendio	3	2	2	2	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	1	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	2	2	2	4	MB

	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	2	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
DELL NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	3	2	2	2	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	1	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	1	2	2	2	2	MB
	No existe control sobre las personas que ingresan y salen de la organización	Robo	2	2	2	2	4	MB
	Falta de conexiones seguras	Error en la manipulación de las redes	4	2	2	2	8	B
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	4	2	2	2	8	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	2	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	1	1	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	2	2	2	8	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	2	2	6	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	2	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	4	2	2	2	8	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	2	2	2	4	MB

	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	1	1	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	2	2	2	8	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	3	2	2	2	6	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	2	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	3	2	2	2	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	1	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	2	2	2	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	2	2	8	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	2	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	3	2	2	2	6	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	2	2	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	1	1	1	3	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	2	2	2	8	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	2	2	2	8	B
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	2	2	10	M

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	2	2	2	2	4	MB
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	1	1	1	4	MB
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	3	2	2	2	6	B
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	2	2	10	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	2	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	4	2	2	2	8	B
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	3	2	2	2	6	B
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	1	1	1	5	B
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	5	2	2	2	10	M
	No existe control sobre las personas que ingresan y salen de la organización	Robo	5	2	2	2	10	M
	Falta de conexiones seguras	Error en la manipulación de las redes	5	2	2	2	10	M
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	2	2	2	2	4	MB
S.O Windows	Errores en la configuración de seguridad	Ciberataques	5	3	2	3	15	A
	Asignación errada en los accesos	Abuso de los equipos	4	1	2	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	3	3	3	12	M
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	2	2	2	8	B

	Interfaces de difícil manipulación	Errores de uso	2	2	2	2	4	MB
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	3	3	3	12	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	3	3	3	15	A
	No existencia de copias de seguridad	Mal funcionamiento del software	2	3	3	3	6	B
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	5	2	2	2	10	M
	Asignación errada en los accesos		4	1	2	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	3	3	3	12	M
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	2	2	2	8	B
	Interfaces de difícil manipulación	Errores de uso	2	2	2	2	4	MB
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	3	3	3	3	9	B
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	3	3	3	15	A
	No existencia de copias de seguridad	Mal funcionamiento del software	2	3	3	3	6	B
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	5	2	2	2	10	M
	Asignación errada en los accesos	Abuso de los equipos	4	1	2	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	4	3	3	3	12	M
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	2	2	2	8	B
	Interfaces de difícil manipulación	Errores de uso	2	2	2	2	4	MB
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	3	3	3	12	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	3	3	3	15	A
	No existencia de copias de seguridad	Mal funcionamiento del software	2	3	3	3	6	B

Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	5	2	2	2	10	M
	Asignación errada en los accesos	Abuso de los equipos	4	1	2	2	8	B
	Ausencia de documentación de uso	Modificación sin autorización	5	3	3	3	15	A
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	2	3	3	12	M
	Interfaces de difícil manipulación	Errores de uso	2	2	3	3	6	B
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	3	3	3	12	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	3	3	3	15	A
	No existencia de copias de seguridad	Mal funcionamiento del software	2	3	3	3	6	B
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	2	2	2	0	MB
	Asignación errada en los accesos	Abuso de los equipos	0	1	2	2	0	MB
	Ausencia de documentación de uso	Modificación sin autorización	4	3	3	3	12	M
	Inadecuada utilización de los sistemas	Errores de mantenimiento	4	2	2	2	8	B
	Interfaces de difícil manipulación	Errores de uso	2	2	2	2	4	MB
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	4	3	3	3	12	M
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	5	3	3	3	15	A
	No existencia de copias de seguridad	Mal funcionamiento del software	2	3	3	3	6	B
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	3	2	3	15	A
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	3	2	3	9	B

	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	3	3	3	15	A
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	3	2	3	12	M
	No existencia de políticas de mensajería	Perdida de los datos	2	4	3	4	8	B
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	4	3	4	20	MA
Personal de planta (técnicos, secretarias, contadores , gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	5	2	2	2	10	M
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	3	3	2	3	9	B
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	5	3	3	3	15	A
	Entrenamiento insuficiente del personal	Perdida de personal clave	4	3	2	3	12	M
	No existencia de políticas de mensajería	Perdida de los datos	4	4	3	4	16	A
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	5	4	3	4	20	MA
Bases de datos	Inadecuada administración de los datos	Fuga de información	5	3	3	3	15	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	3	2	2	2	6	B
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	3	2	2	2	6	B
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	2	2	2	10	M
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	3	2	2	2	6	B
	No existencia de copias de respaldo	Perdida de información	5	3	3	3	15	A
Documentos	Inadecuada administración de los datos	Fuga de información	5	3	3	3	15	A
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	2	2	2	2	4	MB

compartidos	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	2	2	10	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	2	2	2	10	M
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	2	2	2	4	MB
	No existencia de copias de respaldo	Perdida de información	5	3	3	3	15	A
Balances	Inadecuada administración de los datos	Fuga de información	4	3	3	3	12	M
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	2	2	2	8	B
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	5	2	2	2	10	M
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	5	2	2	2	10	M
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	2	2	2	2	4	MB
	No existencia de copias de respaldo	Perdida de información	5	3	2	3	15	A
Planillas de pago	Falta de protecciones contra incendios	Incendio	5	2	3	3	15	A
	Falta de instalaciones correctas	Daños por agua	5	2	2	2	10	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	5	1	3	2	10	M
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	2	2	2	10	M
Planillas de servicios	Falta de protecciones contra incendios	Incendio	4	2	3	3	12	M
	Falta de instalaciones correctas	Daños por agua	5	2	2	2	10	M
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	1	3	2	8	B
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	2	2	2	10	M

Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	4	2	3	3	12	M
	Falta de instalaciones correctas	Daños por agua	4	2	2	2	8	B
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	1	3	2	8	B
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	2	2	2	10	M
Información de los servicios	Falta de protecciones contra incendios	Incendio	4	2	3	3	12	M
	Falta de instalaciones correctas	Daños por agua	4	2	2	2	8	B
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	1	3	2	8	B
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	2	2	2	10	M
Diagramas de red	Falta de protecciones contra incendios	Incendio	5	2	3	3	15	A
	Falta de instalaciones correctas	Daños por agua	5	2	3	3	15	A
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	4	1	3	2	8	B
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	5	2	2	2	10	M
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	5	3	3	3	15	A
	Ausencia de protecciones digitales	Perdida de equipos	4	0	2	1	4	MB
	Ubicación en área susceptible a desastres	Desastres naturales	3	2	2	2	6	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	3	2	2	2	6	B
	Perdida de información	Destrucción de los equipos	5	2	2	2	10	M
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	3	3	3	6	B
	Ausencia de protecciones digitales	Perdida de equipos	4	0	2	1	4	MB
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	2	2	8	B

	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	2	2	2	4	MB
	Perdida de información	Destrucción de los equipos	5	2	2	2	10	M
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	2	2	3	3	6	B
	Ausencia de protecciones digitales	Perdida de equipos	3	0	2	1	3	MB
	Ubicación en área susceptible a desastres	Desastres naturales	4	2	2	2	8	B
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	2	2	2	2	4	MB
	Perdida de información	Destrucción de los equipos	5	2	2	2	10	M
Correo	Interfaz de usuarios complejas	Error en el uso	5	0	1	1	5	B
	Gestión deficiente de contraseñas	Vulneración de la sesión	5	2	2	2	10	M
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	4	3	2	3	12	M
	Líneas de comunicación sin protección	Filtración de información	4	1	1	1	4	MB
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	3	1	1	1	3	MB
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	3	1	1	1	3	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	2	2	2	8	B
	Monitoreo inadecuado de las instalaciones	Robo	5	2	2	2	10	M
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	1	1	2	MB
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	1	1	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	2	2	2	4	MB

	Monitoreo inadecuado de las instalaciones	Robo	2	2	2	2	4	MB
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	1	1	2	MB
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	1	1	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	2	2	2	4	MB
	Monitoreo inadecuado de las instalaciones	Robo	2	2	2	2	4	MB
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	1	1	2	MB
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	2	1	1	1	2	MB
	No se posee sistema de refrigeración actual	Fallos en los equipos	2	2	2	2	4	MB
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	2	2	2	2	4	MB
	Monitoreo inadecuado de las instalaciones	Robo	2	2	2	2	4	MB
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	1	1	1	2	MB

Anexo 16. Declaración de aplicabilidad de los controles

Dominio	Objetivos de control	Controles	Aplicabilidad	Justificación
A.5. Políticas de Seguridad de la Información	A.5.1. Directrices de la Dirección en Seguridad de la Información	A.5.1.1. Conjunto de políticas para la seguridad de la información	Si	Se debe crear un conjunto de políticas para la seguridad de la información las cuales sean aprobadas por la Dirección y posterior a ello deben ser publicadas y comunicadas a los empleados y partes interesadas de la empresa.

		A.5.1.2. Revisión de las políticas para la seguridad de la información	Si	Las políticas de seguridad de la Información deben ser revisadas en intervalos de tiempo para asegurar la eficacia de las mismas.
A.6. Aspectos Organización de la Seguridad de la Información	A.6.1. Organización Interna	A.6.1.1. Funciones y responsabilidades de la seguridad de la información	Si	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
		A.6.1.2. Segregación de tareas	Si	Las áreas y tareas se deben separar para reducir las posibilidades de modificación no autorizada o el uso indebido de los activos de la organización.
		A.6.1.3. Contacto con las autoridades	Si	Se debe mantener un contacto apropiados con las autoridades.
		A.6.1.4. Contacto con grupos de interés especial	Si	Se debería mantener una comunicación con grupos, foros y asociaciones profesionales las cuales estén especializadas en seguridad.
		A.6.1.5. Seguridad de la información en la gestión de proyectos	Si	Se debe gestionar de forma correcta la seguridad de la información de los proyectos independiente de su tipo.
	A.6.2. Dispositivos Móviles y Teletrabajo	A.6.2.1. Política de uso de dispositivos móviles	Si	Se deben adoptar una política de seguridad la cual ayude a gestionar los riesgos que se pueden generar por el uso los dispositivos móviles.
		A.6.2.2. Teletrabajo	Si	Se deben implementar una política de seguridad la cual ayude a proteger la información a la que se tiene acceso cuando se realiza teletrabajo.
A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.1. Investigación de antecedentes	Si	Se debe realizar la verificación de los antecedentes de todos los candidatos a ser empleado de acuerdo con las leyes y reglamentos pertinentes.
		A.7.1.2. Términos y condiciones de contratación	Si	En los acuerdos que se realiza con los empleados y contratistas se debe establecer sus responsabilidades y las de la organización en lo referente a seguridad de la información.
	A.7.2. Durante la	A.7.2.1. Responsabilidades de gestión	Si	La dirección debe exigir a todos los empleados y contratistas la aplicación de las

	contratación			políticas y procedimientos establecidos de la organización.
		A.7.2.2. Concienciación, educación y capacitación en seguridad de la información	Si	Todos los empleados de la organización y los contratistas deben recibir educación apropiada sobre las políticas pertinentes para su cargo.
		A.7.2.3. Proceso disciplinario	Si	Se debe poseer un proceso formal el cual permita emprender acciones contra los empleados que hayan realizado una violación a la seguridad de la información.
	A.7.3. Cese o cambio de puesto de trabajo	A.7.3.1. Cese o cambio de puesto de trabajo	Si	Se deben definir y comunicar al empleado o contratista los deberes y responsabilidades de seguridad de la información que debe cumplir después de la terminación o cambio de empleo.
A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.1. Inventario de activos	Si	Se deben identificar todos los activos que posee la empresa, también se debe elaborar y mantener actualizado el inventario de estos activos.
		A.8.1.2. Propiedad de los activos	Si	Todos los activos mantenidos en el inventario deben ser propios.
		A.8.1.3. Uso aceptable de los activos	Si	Se deben implementar reglas para el uso aceptable de los activos asociados con información.
		A.8.1.4. Devolución de activos	Si	Al terminar su empleo o contrato todos los empleados y usuarios externos deben devolver los activos que se encuentren a su cargo.
	A.8.2. Clasificación de la información	A.8.2.1. Directrices de clasificación	Si	Se debe clasificar la información según los requisitos legales, criticidad, susceptibilidad a ser divulgada y a modificación no autorizada.
		A.8.2.2. Etiquetado y manipulado de la información	Si	Se debe implementar un etiquetado acuerdo de la información empleado el esquema de clasificación que posea la empresa.
		A.8.2.3. Manipulación de activos	Si	Se debe implementar procedimientos adecuados para el manejo de activos según el esquema de clasificación adoptado por la

				empresa.
	A.8.3. Manejo de los soportes de almacenamiento	A.8.3.1. Gestión de medios removibles	Si	Se deben implementar procedimientos para la gestión de medios removibles según el esquema de clasificación adoptado por la empresa.
		A.8.3.2. Eliminación de soportes	Si	Se debe eliminar de forma segura los medios de soporte cuando ya no se los requieran.
		A.8.3.3. Soportes físicos en tránsito	Si	Se deben proteger los soportes físicos durante el transporte para de esta manera impedir el acceso no autorizado, uso indebido o corrupción.
A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.1. Política de control de acceso	Si	Se debe establecer y documentar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
		A.9.1.2. Control de acceso a las redes y servicios asociados	Si	Se debe permitir solo el acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados.
	A.9.2. Gestión de acceso de usuarios	A.9.2.1. Gestión de altas/bajas en el registro de usuarios	Si	Se debe implementar un proceso de registro para tener una correcta asignación de los derechos de acceso.
		A.9.2.2. Gestión de los derechos de acceso asignados a usuarios	Si	Se debe implementar un proceso formal de acceso de usuarios el cual ayude a asignar o cancelar los derechos de acceso a los usuarios para todos los sistemas y servicios
		A.9.2.3. Gestión de derechos de acceso con privilegios especiales	Si	Se debe implementar un registro y control para la asignación y uso de derechos de acceso privilegiado.
		A.9.2.4. Gestión de información confidencial de autenticación de usuarios	Si	La información de autenticación secreta se debe gestionar mediante un procedimiento de gestión formal.
		A.9.2.5. Revisión de los derechos de acceso de usuarios	Si	Los dueños de los activos deben revisar los derechos de acceso de los usuarios.
		A.9.2.6. Cancelación o ajuste de los derechos de acceso	Si	Al terminar su empleo o contrato se deben cancelar los derechos de acceso a la información y a las instalaciones a todos los empleados y de usuarios externos.

	A.9.3. Responsabilidades de los usuarios	A.9.3.1. Uso de información confidencial para la autenticación	Si	Se debe exigir a los usuarios que cumplan las normas de la empresa para el uso correcto de la información de autenticación secreta.
	A.9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1. Restricción de acceso a la información	Si	Se debe restringir el acceso a la información y a las funciones de los sistemas de acuerdo con la política de control de acceso.
		A.9.4.2. Procedimientos seguros de inicio de sesión	Si	Se debe controlar mediante un proceso de conexión segura.
		A.9.4.3. Gestión de contraseñas de usuario	Si	Los sistemas de gestión de contraseñas deben ser interactivos y de fácil manipulación.
		A.9.4.4. Uso de herramientas de administración de sistemas	No	No se posee estos programas en la empresa.
		A.9.4.5. Control de acceso al código fuente de programas	No	La empresa no trabaja con códigos fuente de programas.
A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.1. Política sobre el uso de controles criptográficos	Si	Se debe crear e implementar una política para el uso de controles criptográficos los cuales ayudan a la protección de la información.
		A.10.1.2. Gestión de Claves.	Si	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas
A.11. Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.1. Perímetro de seguridad física	Si	Se deben definir y usar perímetros de seguridad para proteger las áreas que contengan información confidencial o crítica.
		A.11.1.2. Controles físicos de entrada	Si	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
		A.11.1.3. Seguridad de oficinas, despachos y recursos	Si	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa.
		A.11.1.4. Protección contra amenazas externas y ambientales	Si	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes

		A.11.1.5. Trabajo en áreas seguras.	Si	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
		A.11.1.6. Áreas de acceso público, despacho y carga.	Si	Se deben controlar los puntos de acceso para evitar el acceso de personal no autorizado.
	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Si	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados.
		A.11.2.2. Instalaciones de suministro	Si	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos.
		A.11.2.3. Seguridad del cableado	Si	Se debe proteger al cableado contra interferencia o daño.
		A.11.2.4. Mantenimiento de los equipos	Si	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad.
		A.11.2.5. Retiro de bienes	Si	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
		A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	Si	Se deben emplear medidas de seguridad a los activos que se encuentran fuera de la organización.
		A.11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento	Si	Se deben verificar que los medios de almacenamiento hayan sido retirados o sobre escrito de forma segura antes de su reúso.
		A.11.2.8. Equipos desatendidos por los usuarios	Si	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada
		A.11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla	Si	Se debe generar una política de escritorio limpio y de pantalla limpia.
A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Si	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
		A.12.1.2. Gestión de cambios	Si	Se deben controlar los cambios en los procesos de negocio y en los sistemas de

				procesamiento de información ya que estos pueden afectar la seguridad de la información.
		A.12.1.3. Gestión de Capacidad	Si	Se deben realizar proyecciones de los requisitos de capacidad futura, para de esta forma asegurar el desempeño requerido del sistema.
		A.12.1.4. Separación de los ambientes de desarrollo, prueba y producción	No	No se posee ambientes de desarrollo.
	A.12.2. Protección contra códigos maliciosos	A.12.2.1. Controles contra códigos maliciosos	Si	Se deben implementar controles de detección, de prevención y de recuperación para proteger a los activos contra códigos maliciosos.
	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Si	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
	A.12.4. Registro de actividad y supervisión	A.12.4.1. Registro de eventos.	Si	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información
		A.12.4.2. Protección de los registros de información	Si	Se deben proteger contra alteración y acceso no autorizado a las instalaciones y la información de registro
		A.12.4.3. Registros de actividad del administrador y operador del sistema	Si	Se deben registrar las actividades del administrador y del operador del sistema y estos registros se deben proteger y revisar con regularidad
		A.12.4.4. Sincronización de relojes	Si	Los relojes de todos los sistemas de procesamiento de información se deben sincronizar con una única fuente de referencia de tiempo
	A.12.5. Control de software en la producción	A.12.5.1. Instalación de software en sistemas operativos	Si	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos

	A.12.6. Gestión de vulnerabilidad técnica	A.12.6.1. Gestión de las vulnerabilidades técnicas	Si	Se debe obtener de forma oportuna información sobre las vulnerabilidades técnicas de los sistemas de información y evaluar la exposición de la organización a estas vulnerabilidades, posterior a ello tomar las medidas apropiadas para tratar el riesgo asociado
		A.12.6.2. Restricciones sobre la instalación de software	Si	Se debe establecer e implementar un reglamento de instalación de software por parte de los usuarios
	A.12.7. Consideraciones de las auditorías de los sistemas de información	A.12.7.1. Controles de auditorías de los sistemas de información	No	Se trata de auditorías técnicas sobre el sistema para evaluar cosas como: los usuarios están trabajando con los privilegios correctos, la infraestructura es estable y confiable, etc.
A.13. Seguridad de las Comunicaciones	A.13.1. Gestión de Seguridad en las redes	A.13.1.1. Controles de redes	Si	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones
		A.13.1.2. Seguridad de los servicios de red	Si	Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red ya sea que los servicios se presten de forma internamente o externa
		A.13.1.3. Separación en las redes	Si	Se deben separar los grupos de servicios de información, usuarios y sistemas de información
	A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	Si	Se debe contar con políticas, procedimientos y controles de transferencia para proteger la información que se va a trasmitir
		A.13.2.2. Acuerdos de intercambio de información	Si	Debe haber acuerdos entre la organización y las partes externas para poder garantizar el uso de la información
		A.13.2.3. Mensajería electrónica	Si	Se debe incluir controles apropiados para proteger la información que se incluye en los mensajes electrónicos
		A.13.2.4. Acuerdos de confidencialidad y de no divulgación	Si	Se deben identificar y documentar los acuerdos de confidencialidad y no divulgación de la organización para la

				protección de la información
A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.1. Requisitos de seguridad de los sistemas de información	A.14.1.1. Análisis y especificación de los requisitos de seguridad de la información	Si	Los requisitos de seguridad se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información ya existentes
		A.14.1.2. Aseguramiento de los servicios de aplicaciones en las redes públicas	Si	Si utilizamos redes públicas para trasmitir información se debe implementar controles para proteger de actividades fraudulentas, divulgación y modificación no autorizadas
		A.14.1.3. Protección de las transacciones en línea	Si	Se trata de implementar controles que garanticen la protección de las transacciones entre aplicaciones
	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.1. Política de desarrollo seguro de software	No	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización
		A.14.2.2. Procedimiento de control de cambios en los sistemas	No	Se deben establecer reglas para los cambios que se generen en dentro del ciclo de vida de desarrollo de software y de sistemas
		A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	Si	Cuando se cambian los sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
		A.14.2.4. Restricciones sobre los cambios de paquetes de software	Si	Se deben limitar las modificaciones a los paquetes de software para poder minimizar la generación de incidentes
		A.14.2.5. Uso de principios de ingeniería en protección de sistemas	Si	Se deben establecer y documentar principios de sistemas seguros y aplicarlos a cualquier trabajo de implementación de sistemas de información.
		A.14.2.6. Ambiente de desarrollo seguro	No	No se posee ambientes de desarrollo.
		A.14.2.7. Externalización del desarrollo de software	No	No se realiza actividad de desarrollo de sistemas subcontratados.
		A.14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas	No	En la empresa no se realiza desarrollo.

		A.14.2.9. Pruebas de aceptación de sistemas	Si	Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados
	A.14.3. Datos de prueba	A.14.3.1. Protección de los datos utilizados en pruebas	Si	Los datos de pruebas se deben seleccionar, proteger y controlar cuidadosamente.
A.15. Relaciones con los Proveedores	A.15.1. Seguridad de la información en las relaciones con los proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores	Si	Se deben acordar con los proveedores regulaciones las cuales ayuden a mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización
		A.15.1.2. Tratamiento del riesgo dentro de los acuerdos con los proveedores	Si	Se deben establecer y generar todos documentos pertinentes con cada proveedor que puedan tener acceso a la información de la organización
		A.15.1.3. Cadena de suministro en tecnologías de información y comunicación	Si	Los acuerdos con proveedores deben incluir información asociados con el manejo correcto de la cadena de suministro de productos y servicios de tecnología de información y comunicación
	A.15.2. Gestión de la prestación de servicios de proveedores	A.15.2.1. Supervisión y revisión de los servicios prestados por terceros	Si	Se debe establecer mecanismos de monitorización de los servicios proporcionados por terceros y además solicitar los informes al proveedor sobre el servicio prestado
		A.15.2.2. Gestión de cambios en los servicios de los proveedores	Si	Se deben gestionar los cambios en el suministro de servicios teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados.
A.16. Gestión de Incidentes de Seguridad de la Información	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1. Responsabilidades y procedimientos	Si	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida y eficaz a los incidentes de seguridad
		A.16.1.2. Notificación de los eventos de seguridad de la información	Si	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible
		A.16.1.3. Notificación de puntos débiles de la seguridad	Si	Se debe exigir a todos los que usan los servicios y sistemas de información que

				informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios
		A.16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones	Si	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes
		A.16.1.5. Respuesta a incidentes de seguridad de seguridad	Si	Se debe dar respuesta a los incidentes de seguridad de acuerdo con los procedimientos documentados
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	Si	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros
		A.16.1.7. Recolección de evidencia	Si	Se debe definir y aplicar procedimientos para la identificación, recolección y preservación de información que puede servir como evidencia
A.17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	A.17.1. Continuidad de la seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información	Si	En este control se debe tener integrados los requisitos de la seguridad de la información en los planes de continuidad del negocio determinando
		A.17.1.2. Implementación de la continuidad de la seguridad de la información	Si	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si	La organización debe verificar los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que sean eficaces durante situaciones adversas
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información	Si	Las instalaciones de procesamiento de información se deben implementar con redundancia para cumplir los requisitos de disponibilidad
	A.18.1. Cumplimiento de los	A.18.1.1. Identificación de la legislación aplicable	Si	Se deben identificar, documentar y mantener actualizados todos los requisitos legislativos,

A.18. Cumplimiento	requisitos legales y contractuales			de reglamentación y contractuales pertinentes
		A.18.1.2. Derechos de Propiedad Intelectual	No	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los reglamentos relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados
		A.18.1.3. Protección de los registros de la organización	Si	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada
		A.18.1.4. Protección de datos y privacidad de la información personal	Si	Se deben asegurar la privacidad y la protección de la información personal como se exige en la legislación y la reglamentación
		A.18.1.5. Regulación de los controles criptográficos	Si	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información	Si	Se deben ser realizar revisiones por personal independiente al personal que es auditado. Aunque pueden ser llevadas a cabo por personal interno siempre de áreas o departamentos independientes al auditado
		A.18.2.2. Cumplimiento de las políticas y normas de seguridad	Si	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad
		A.18.2.3. Revisión del cumplimiento técnico	Si	Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información

Anexo 17. Selección de objetivos de control y controles

Nombre del Activo	Vulnerabilidades	Amenazas	Valor del riesgo residual	Magnitud del riesgo	Dominio	Objetivos de control	Controles	Justificación de aplicabilidad
Laptops	Falta de mantenimiento en el sistema antiincendios	Incendio	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad

	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	8	B	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Falta de mantenimiento en el sistema antiincendios	Incendio	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas	Se debe diseñar y aplicar protección física contra desastres

Pcs Escritorio							externas y ambientales	naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y

								recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	8	B	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
NUC	Falta de mantenimiento en el sistema antiincendios	Incendio	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos

	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	2	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	4	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	8	B	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el

						de los equipos		suministro necesario para poder mantener operativas las instalaciones y los equipos
Servidores DELL R240	Falta de mantenimiento en el sistema antiincendios	Incendio	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y

								peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
Servidores DELL R230	Falta de mantenimiento en el sistema antiincendios	Incendio	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes

	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	A.9. Control de Acceso	A.9.1. Requisitos del negocio	A.9.1.2. Control de acceso a las	Solo se debe permitir acceso de los usuarios a

						para el control de acceso	redes y servicios asociados	la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
FIREWALL	Falta de mantenimiento en el sistema antiincendios	Incendio	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente

								para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos

Router MIKROTIK	Falta de mantenimiento en el sistema antiincendios	Incendio	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	3	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados

	No existe control sobre las personas que ingresan y salen de la organización	Robo	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
Switch	Falta de mantenimiento en el sistema antiincendios	Incendio	4	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las

								instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el almacenamiento de los equipos	Robo	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	10	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente

	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
Switch de CORE	Falta de mantenimiento en el sistema antiincendios	Incendio	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee un amplio sistema de refrigeración	Sobrecalentamiento y daño de los equipos en el data center	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Descompostura de los equipos por error en la manipulación	5	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
	No existe medidas adecuadas para el	Robo	10	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad	A.11.2.1. Ubicación y	Los equipos deben estar ubicados y

	almacenamiento de los equipos					de los equipos	protección de los equipos	protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existe control sobre las personas que ingresan y salen de la organización	Robo	10	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.3. Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física a oficinas, despachos y recursos que posee la empresa
	Falta de conexiones seguras	Error en la manipulación de las redes	10	M	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.2. Control de acceso a las redes y servicios asociados	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	Fallo en el suministro de energía eléctrica	Perdida de servicio de internet total	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
S.O Windows	Errores en la configuración de seguridad	Ciberataques	15	A	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.3. Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información,

								activos de información e instalaciones de procesamiento de información
	Asignación errada en los accesos	Abuso de los equipos	8	B	A.9. Control de Acceso	A.9.2. Gestión de acceso de usuarios	A.9.2.2. Gestión de los derechos de acceso asignados a usuarios	Se debe implementar un proceso formal de acceso de usuarios el cual ayude a asignar o cancelar los derechos de acceso a los usuarios para todos los sistemas y servicios
	Ausencia de documentación de uso	Modificación sin autorización	12	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	Inadecuada utilización de los sistemas	Errores de mantenimiento	8	B	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.4. Restricciones sobre los cambios de paquetes de software	Se deben limitar las modificaciones a los paquetes de software para poder minimizar la generación de incidentes
	Interfaces de difícil manipulación	Errores de uso	4	MB	A.14. Adquisición,	A.14.2. Seguridad	A.14.2.3. Revisión	Cuando se cambian los

					Desarrollo y Mantenimiento de Sistemas	en los procesos de desarrollo y soporte	técnica de las aplicaciones después de efectuar cambios en el sistema operativo	sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	12	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.8. Equipos desatendidos por los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	15	A	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.2. Gestión de Claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas
	No existencia de copias de seguridad	Mal funcionamiento del software	6	B	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias

								de respaldo establecidas
S.O Ubuntu	Errores en la configuración de seguridad	Ciberataques	10	M	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.3. Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información, activos de información e instalaciones de procesamiento de información
	Asignación errada en los accesos		8	B	A.9. Control de Acceso	A.9.2. Gestión de acceso de usuarios	A.9.2.2. Gestión de los derechos de acceso asignados a usuarios	Se debe implementar un proceso formal de acceso de usuarios el cual ayude a asignar o cancelar los derechos de acceso a los usuarios para todos los sistemas y servicios
	Ausencia de documentación de uso	Modificación sin autorización	12	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	Inadecuada utilización de los sistemas	Errores de mantenimiento	8	B	A.14.	A.14.2. Seguridad	A.14.2.4. Restriccione	Se deben limitar las

					Adquisición, Desarrollo y Mantenimiento de Sistemas	en los procesos de desarrollo y soporte	s sobre los cambios de paquetes de software	modificaciones a los paquetes de software para poder minimizar la generación de incidentes
	Interfaces de difícil manipulación	Errores de uso	4	MB	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	Cuando se cambian los sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	9	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.8. Equipos desatendidos por los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	15	A	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.2. Gestión de Claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas.
	No existencia de copias de seguridad	Mal funcionamiento del software	6	B	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de	Se deben realizar respaldo de la información, software e

							la información	imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
Software de administración de red U2000	Errores en la configuración de seguridad	Ciberataques	10	M	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.3. Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información, activos de información e instalaciones de procesamiento de información
	Asignación errada en los accesos	Abuso de los equipos	8	B	A.9. Control de Acceso	A.9.2. Gestión de acceso de usuarios	A.9.2.2. Gestión de los derechos de acceso asignados a usuarios	Se debe implementar un proceso formal de acceso de usuarios el cual ayude a asignar o cancelar los derechos de acceso a los usuarios para todos los sistemas y servicios
	Ausencia de documentación de uso	Modificación sin autorización	12	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y	A.12.1.1. Documentación de procedimien	Los procedimientos operativos se deben documentar y

						responsabilidades	tos de operación	poner a disposición de todos los usuarios que los necesitan
	Inadecuada utilización de los sistemas	Errores de mantenimiento	8	B	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.4. Restricciones sobre los cambios de paquetes de software	Se deben limitar las modificaciones a los paquetes de software para poder minimizar la generación de incidentes
	Interfaces de difícil manipulación	Errores de uso	4	MB	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	Cuando se cambian los sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	12	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.8. Equipos desatendidos por los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	15	A	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.2. Gestión de Claves.	Se debe desarrollar e implementar una política sobre el

								uso, protección y tiempo de vida de claves criptográficas.
	No existencia de copias de seguridad	Mal funcionamiento del software	6	B	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
Sistema contable Trantor	Errores en la configuración de seguridad	Ciberataques	10	M	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.3. Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información, activos de información e instalaciones de procesamiento de información
	Asignación errada en los accesos	Abuso de los equipos	8	B	A.9. Control de Acceso	A.9.2. Gestión de acceso de usuarios	A.9.2.2. Gestión de los derechos de acceso asignados a usuarios	Se debe implementar un proceso formal de acceso de usuarios el cual ayude a asignar o cancelar los derechos de acceso a los usuarios para

								todos los sistemas y servicios
	Ausencia de documentación de uso	Modificación sin autorización	15	A	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	Inadecuada utilización de los sistemas	Errores de mantenimiento	12	M	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.4. Restricciones sobre los cambios de paquetes de software	Se deben limitar las modificaciones a los paquetes de software para poder minimizar la generación de incidentes
	Interfaces de difícil manipulación	Errores de uso	6	B	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	Cuando se cambian los sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	12	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad	A.11.2.8. Equipos desatendidos	Los usuarios deben asegurarse de que el equipo

						de los equipos	por los usuarios	sin supervisión tenga la protección apropiada
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	15	A	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.2. Gestión de Claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas.
	No existencia de copias de seguridad	Mal funcionamiento del software	6	B	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
Office 2010	Errores en la configuración de seguridad	Ciberataques	0	MB	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.3. Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información, activos de información e instalaciones de procesamiento de información
	Asignación errada en los accesos	Abuso de los equipos	0	MB	A.9. Control de Acceso	A.9.2. Gestión de	A.9.2.2. Gestión de	Se debe implementar un

						acceso de usuarios	los derechos de acceso asignados a usuarios	proceso formal de acceso de usuarios el cual ayude a asignar o cancelar los derechos de acceso a los usuarios para todos los sistemas y servicios
	Ausencia de documentación de uso	Modificación sin autorización	12	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	Inadecuada utilización de los sistemas	Errores de mantenimiento	8	B	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.4. Restricciones sobre los cambios de paquetes de software	Se deben limitar las modificaciones a los paquetes de software para poder minimizar la generación de incidentes
	Interfaces de difícil manipulación	Errores de uso	4	MB	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	Cuando se cambian los sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso

								en las operaciones o seguridad de la organización
	Falta de bloqueo del equipo al abandonar el puesto de trabajo	Abuso de los equipos	12	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.8. Equipos desatendidos por los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada
	Gestión deficiente al guardar las contraseñas	Mal uso de los equipos	15	A	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.2. Gestión de Claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas.
	No existencia de copias de seguridad	Mal funcionamiento del software	6	B	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
Personal temporal (pasantes)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	15	A	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de

								todos los usuarios que los necesitan
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	9	B	A.18. Cumplimiento	A.18.2. Revisiones de seguridad de la información	A.18.2.3. Revisión del cumplimiento técnico	Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	15	A	A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.1. Investigación de antecedentes	Las verificaciones de los antecedentes de los candidatos a un empleo deben ser llevadas a cabo de acuerdo con las leyes, reglamentos y ética pertinentes
	Entrenamiento insuficiente del personal	Perdida de personal clave	12	M	A.7. Seguridad Ligada a los Recursos Humanos	A.7.2. Durante la contratación	A.7.2.2. Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y los contratistas deben recibir educación sobre las políticas y procedimientos pertinentes para su cargo
	No existencia de políticas de mensajería	Perdida de los datos	8	B	A.13. Seguridad de las Comunicaciones	A.13.2. Transferencia de información	A.13.2.3. Mensajería electrónica	Se debe incluir controles apropiados para proteger la información que se incluye en los

								mensajes electrónicos
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	20	MA	A.7. Seguridad Ligada a los Recursos Humanos	A.7.2. Durante la contratación	A.7.2.2. Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y los contratistas deben recibir educación sobre las políticas y procedimientos pertinentes para su cargo
Personal de planta (técnicos, secretarias, contadores, gerencia)	Ausencia de políticas para tener un correcto uso de los equipos	Robo de documentación	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	No se posee mecanismos de monitoreo sobre el uso de los equipos	Uso no autorizado de los equipos	9	B	A.18. Cumplimiento	A.18.2. Revisiones de seguridad de la información	A.18.2.3. Revisión del cumplimiento técnico	Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información
	Ausencia de personal calificado	Mala manipulación o destrucción de los equipos	15	A	A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.1. Investigación de antecedentes	Las verificaciones de los antecedentes de los candidatos a un empleo deben ser llevadas a cabo de acuerdo

								con las leyes, reglamentos y ética pertinentes
	Entrenamiento insuficiente del personal	Perdida de personal clave	12	M	A.7. Seguridad Ligada a los Recursos Humanos	A.7.2. Durante la contratación	A.7.2.2. Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y los contratistas deben recibir educación sobre las políticas y procedimientos pertinentes para su cargo
	No existencia de políticas de mensajería	Perdida de los datos	16	A	A.13. Seguridad de las Comunicaciones	A.13.2. Transferencia de información	A.13.2.3. Mensajería electrónica	Se debe incluir controles apropiados para proteger la información que se incluye en los mensajes electrónicos
	Falta de conciencia y capacitación sobre la seguridad	Error en el uso	20	MA	A.7. Seguridad Ligada a los Recursos Humanos	A.7.2. Durante la contratación	A.7.2.2. Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y los contratistas deben recibir educación sobre las políticas y procedimientos pertinentes para su cargo
Bases de datos	Inadecuada administración de los datos	Fuga de información	15	A	A.13. Seguridad de las Comunicaciones	A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia para proteger la información que se va a trasmitir

	Falta de protecciones físicas adecuadas	Daños por agua o fuego	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	6	B	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	10	M	A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.2. Términos y condiciones de contratación	Los acuerdos con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los

								accesos no autorizados
	No existencia de copias de respaldo	Perdida de información	15	A	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
Documentos compartidos	Inadecuada administración de los datos	Fuga de información	15	A	A.13. Seguridad de las Comunicaciones	A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia para proteger la información que se va a trasmitir
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	4	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los

								usuarios que los necesitan
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	10	M	A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.2. Términos y condiciones de contratación	Los acuerdos con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información
	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existencia de copias de respaldo	Perdida de información	15	A	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas

Balances	Inadecuada administración de los datos	Fuga de información	12	M	A.13. Seguridad de las Comunicaciones	A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia para proteger la información que se va a trasmitir
	Falta de protecciones físicas adecuadas	Daños por agua o fuego	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de conocimientos por parte del personal	No se posee una correcta documentación de los procesos pagos	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
	Falta de plan de continuidad del negocio	Contratos de forma incompleta	10	M	A.7. Seguridad Ligada a los Recursos Humanos	A.7.1. Antes de la contratación	A.7.1.2. Términos y condiciones de contratación	Los acuerdos con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información

	Ubicación inadecuada de los recursos físicos los cuales pueden ser afectados por los desastres naturales	Desastres naturales	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	No existencia de copias de respaldo	Perdida de información	15	A	A.12. Seguridad de las Operaciones	A.12.3. Copias de seguridad	A.12.3.1. Copias de seguridad de la información	Se deben realizar respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba de forma regular de acuerdo con una política de copias de respaldo establecidas
Planillas de pago	Falta de protecciones contra incendios	Incendio	15	A	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de instalaciones correctas	Daños por agua	10	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques

								maliciosos o accidentes
	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	10	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
Planillas de servicios	Falta de protecciones contra incendios	Incendio	12	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de instalaciones correctas	Daños por agua	10	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes

	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
Ordenes de trabajo	Falta de protecciones contra incendios	Incendio	12	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de instalaciones correctas	Daños por agua	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes

	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
Información de los servicios	Falta de protecciones contra incendios	Incendio	12	M	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de instalaciones correctas	Daños por agua	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes

	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
Diagramas de red	Falta de protecciones contra incendios	Incendio	15	A	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Falta de instalaciones correctas	Daños por agua	15	A	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes

	Condiciones locales que pueden afectar las instalaciones	Desastres naturales	8	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
	Ausencia de políticas para tener un correcto almacenamiento de la documentación	Robo de documentación	10	M	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Documentación de procedimientos de operación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan
Edificios	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	15	A	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.1. Política de control de acceso	Se debe establecer y documentar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
	Ausencia de protecciones digitales	Perdida de equipos	4	MB	A.11. Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.2. Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se

								permite el acceso a personal autorizado
	Ubicación en área susceptible a desastres	Desastres naturales	6	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	6	B	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Perdida de información	Destrucción de los equipos	10	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
Vehículos	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	6	B	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.1. Política de control de acceso	Se debe establecer y documentar una política de control de acceso con base en los requisitos del negocio y de

								seguridad de la información
	Ausencia de protecciones digitales	Perdida de equipos	4	MB	A.11. Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.2. Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado
	Ubicación en área susceptible a desastres	Desastres naturales	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Perdida de información	Destrucción de los equipos	10	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su

								integridad y disponibilidad
Antenas	Pueden ingresar personal de áreas no autorizadas	Acceso no autorizado	6	B	A.9. Control de Acceso	A.9.1. Requisitos del negocio para el control de acceso	A.9.1.1. Política de control de acceso	Se debe establecer y documentar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
	Ausencia de protecciones digitales	Perdida de equipos	3	MB	A.11. Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.2. Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado
	Ubicación en área susceptible a desastres	Desastres naturales	8	B	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	Redes eléctricas inestables	Cambios de voltaje o perdidas de energía	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las

								instalaciones y los equipos
	Perdida de información	Destrucción de los equipos	10	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.4. Mantenimiento de los equipos	Son controles que ayudan a garantizar que los equipos se mantienen de forma correctamente para asegurar su integridad y disponibilidad
Correo	Interfaz de usuarios complejas	Error en el uso	5	B	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.3. Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	Cuando se cambian los sistemas operativos se debe revisar y probar las aplicaciones para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
	Gestión deficiente de contraseñas	Vulneración de la sesión	10	M	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.2. Gestión de Claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas
	No finalización de la sesión cuando se abandona el lugar de trabajo	Abuso de los derechos	12	M	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.8. Equipos desatendidos por los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la

								protección apropiada
	Líneas de comunicación sin protección	Filtración de información	4	MB	A.13. Seguridad de las Comunicaciones	A.13.1. Gestión de Seguridad en las redes	A.13.1.2. Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red ya sea que los servicios se presten de forma internamente o externa
	Ausencia de autentificación del emisor y del receptor	Corrupción de datos	3	MB	A.13. Seguridad de las Comunicaciones	A.13.1. Gestión de Seguridad en las redes	A.13.1.1. Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones
Control de acceso	Falta de mantenimiento en el sistema antiincendios	Incendio	3	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee sistema de refrigeración actual	Fallos en los equipos	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las

								instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	8	B	A.8. Gestión de Activos	A.8.2. Clasificación de la información	A.8.2.3. Manipulación de activos	Se deben desarrollar e implementar procedimientos apropiados para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
	Monitoreo inadecuado de las instalaciones	Robo	10	M	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.5. Retiro de bienes	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
UPS	Falta de mantenimiento en el sistema antiincendios	Incendio	2	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques

								maliciosos o accidentes
	No se posee sistema de refrigeración actual	Fallos en los equipos	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	MB	A.8. Gestión de Activos	A.8.2. Clasificación de la información	A.8.2.3. Manipulación de activos	Se deben desarrollar e implementar procedimientos apropiados para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
	Monitoreo inadecuado de las instalaciones	Robo	4	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.5. Retiro de bienes	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales

								también de los accesos no autorizados
Fibra óptica	Falta de mantenimiento en el sistema antiincendios	Incendio	2	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee sistema de refrigeración actual	Fallos en los equipos	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	MB	A.8. Gestión de Activos	A.8.2. Clasificación de la información	A.8.2.3. Manipulación de activos	Se deben desarrollar e implementar procedimientos apropiados para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
	Monitoreo inadecuado de las instalaciones	Robo	4	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.5. Retiro de bienes	Los equipos, información o software no se deben retirar de su sitio sin

								autorización previa.
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados
Aire acondicionado	Falta de mantenimiento en el sistema antiincendios	Incendio	2	MB	A.11.Seguridad Física y Ambiental	A.11.1. Áreas seguras	A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	No se posee sistema de refrigeración actual	Fallos en los equipos	4	MB	A.11.Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.2. Instalaciones de suministro	Se establecen medidas de control para el suministro necesario para poder mantener operativas las instalaciones y los equipos
	Manejo inadecuado de los equipos físicos	Destrucción de los equipos	4	MB	A.8. Gestión de Activos	A.8.2. Clasificación de la información	A.8.2.3. Manipulación de activos	Se deben desarrollar e implementar procedimientos apropiados para el manejo de activos, de acuerdo con el esquema de

								clasificación de información adoptado por la organización
	Monitoreo inadecuado de las instalaciones	Robo	4	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.5. Retiro de bienes	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
	No existe las medidas adecuadas para el almacenamiento de los equipos	Corrosión	2	MB	A.11. Seguridad Física y Ambiental	A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales también de los accesos no autorizados

Anexo 18. Políticas de seguridad para Ultralink

Política de seguridad para controlar el acceso físico y del entorno

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE CONTROL DE ACCESO FÍSICA Y DEL ENTORNO		
OBJETIVO:	Controlar el acceso físico no autorizado, prevenir los daños o robos de los activos de la empresa mediante la utilización de mecanismos de acceso físico o lógico.	
ALCANCE:	La presente política es aplicable a todo el personal, visitantes y proveedores que requieran ingresar a las instalaciones de la empresa	
REFERENCIA:	11.1. Áreas seguras 11.1.1. Perímetro de seguridad física 11.1.2. Controles físicos de entrada 11.1.4. Protección contra amenazas externas y ambientales	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		
• Cuando no exista supervisión verificar que las entradas a las instalaciones estén cerradas de forma correcta. • Toda persona que no pertenezca a la empresa y desee ingresar a las instalaciones de Ultralink debe registrarse y solicitar la autorización de ingreso. • Implementar mecanismos de examinación de bolsos, maletas, cajas, etc. que se deseen ingresar a las instalaciones. • Implementar un monitoreo permanente de los ingresos lo cual ayudara a identificar accesos no autorizados. • Todo el personal de la empresa debe portar su identificación en un lugar visible mientras permanezca dentro de las instalaciones. • Se debe eliminar lo más pronto posible los permisos de acceso físico al personal que termine su vinculación con la empresa • Se debe realizar la devolución del identificador institucional tan pronto se termine la vinculación del personal. • Implementar planes de emergencia o de contingencia ante alguna amenaza externa.		

• Mantener en estado optimo la infraestructura física que posee la empresa, es decir las paredes deben ser sólidas y resistentes. • Separar las áreas que puedan contener activos importantes para la empresa. • Impartir capacitaciones las cuales ayuden a disminuir los riesgos naturales.
RESPONSABILIDADES:
• Todos los coordinadores o supervisores deben asegurarse de que el personal que se encuentre bajo su cargo este informado de forma correcta y le dé cumplimiento a esta política. • Por parte de la gerencia debe proporcionar todas las herramientas que sean necesarias para tener un acceso correcto.

Fuente: [38] [39]

Política para la gestión de los activos

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de control de los activos
POLÍTICA PARA LA GESTIÓN DE LOS ACTIVOS		
OBJETIVO:	Identificar y clasificar de forma correcta los activos que posee la empresa, también definir las responsabilidades para tener una correcta protección de estos.	
ALCANCE:	Esta política está diseñada para el departamento que se encarga de controlar los activos y para todo el personal que usa los activos que posee Ultralink.	
REFERENCIA:	8.1. Responsabilidad sobre los activos. 8.1.1. Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos.	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		
• Se debe generar un inventario de los activos el cual permita organizar y clasificar a los activos según su importancia. • El inventario debe ser actualizado de forma periódica para de esta forma tener un mejor control de los activos. • La información que nos proporcione el inventario debe ser detallada: ubicación, custodio, características del activo, etc.		

• Todos los activos que se encuentren en el inventario deben tener un propietario. • El propietario de los activos debe asegurarse que los activos se encuentren inventariados, clasificados y protegidos. • El propietario de los activos debe garantizar un manejo adecuado del mismo cuando este vaya a ser destruido o eliminado. • Se debe identificar, documentar e implementar reglas para el uso aceptable de los activos que estén asociados con el tratamiento de la información. • Se debe concientizar a los usuarios que tengan accesos a los activos de la organización sobre las normas de seguridad y el tratamiento de la información. • Todos los usuarios de los activos deberán devolver todos los activos que se encuentren en su poder cuando se finalice el contrato o acuerdo de trabajo.
RESPONSABILIDADES:
• Todo usuario que tenga asignado un activo de la empresa tiene la responsabilidad de hacer cumplir las políticas antes mencionadas. • El departamento de tecnología debe implementar los medios necesarios para poder cumplir con esta política.

Fuente: [39] [40]

Política para la gestión de los recursos humanos

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Director de talento humano
POLÍTICA PARA LA GESTIÓN DE LOS RECURSOS HUMANOS		
OBJETIVO:	Hay que asegurar que todo el personal que ingresa y labora en la empresa Ultralink tenga los conocimientos sobre sus deberes, derechos y responsabilidades en materia de seguridad.	
ALCANCE:	Esta política está diseñada para el departamento administrativo, de talento humano y personal técnico que labora en la empresa.	
REFERENCIA:	7.1 Antes de la contratación. 7.2 Durante la contratación. 7.3 Al finalizar la contratación.	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		

- Se deberá realizar una comprobación de los antecedentes de los candidatos para de esta forma verificar que son aptos para los roles a los cuales han sido considerados.
- Para la verificación de los antecedentes se deberá implementar pruebas de habilidades según las necesidades del puesto ofertado.
- Al ser elegido un nuevo integrante en la empresa el nuevo empleado debe firmar un acuerdo de confidencialidad de la información.
- La organización antes de la contratación de los nuevos empleados deberá informar cuales son los roles y responsabilidades que desempeñara en su puesto de trabajo.
- Se debe capacitar al personal en los aspectos relativos a la seguridad de la información.
- Se deberá motivar al personal para que este cumpla con las políticas de seguridad de la información.
- Las capacitaciones que estén relacionadas con la seguridad de la información deben realizarse de forma periódica y de esta forma disminuir los riesgos.
- Cuando se trasfiere a un empleado a un nuevo puesto se debe realizar una capacitación sobre cuáles serían sus nuevos roles y responsabilidades.
- Para poder generar una capacitación eficiente se debe desarrollar un programa el cual este basado en las políticas de seguridad de la empresa.
- Una vez finalizado el contrato el empleado debe cumplir con sus responsabilidades de confidencialidad ya que de no cumplirlas este seria sancionado.
- Cuando se realice un cambio interno en la empresa se debe realizar una actualización de las responsabilidades que tendrá el empleado.

RESPONSABILIDADES:

- El departamento de recursos humanos debe verificar que los antecedentes proporcionados por el postulante sean verídicos.
- Los empleadores deben informar de forma correcta cuales son los roles y responsabilidades que va a tener el empleado.
- El empleado debe leer y comprender cuales son los acuerdos y cláusulas que se estipulan en el contrato antes de firmar.

Fuente: [41] [39]

Política para el control de accesos

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA PARA EL CONTROL DE ACCESOS		
OBJETIVO:	Documentar y establecer todos los controles con respecto al uso de usuarios y contraseñas u otros métodos de autenticación para otorgar permisos de accesos a los sistemas e instalaciones de procesamiento de datos.	
ALCANCE:	Esta política va dirigida para todo el personal de la empresa que requiera contraseñas u otros métodos de autenticación para su acceso.	
REFERENCIA:	9.1. 1. Políticas de control de accesos. 9.2. Gestión de acceso de usuario. 9.3. Responsabilidades del usuario. 9.4. Control de acceso a sistemas y aplicaciones	

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Definir de forma correcta la política para el acceso a la información tomando en cuenta los niveles de seguridad y la clasificación de la información.
- Se debe indicar cuales son los requisitos necesarios para generar la autorización de las solicitudes de acceso.
- Gestionar los accesos de los usuarios teniendo en cuenta la cantidad de privilegios que debe tener cada persona al llevar a cabo las tareas según su puesto de trabajo.
- Cuando se solicite acceso a un sistema de información se debe especificar el tiempo que se necesita para poder cumplir las tareas, caso contrario no se generaran los mismos.
- Se debe generar solo el acceso a aquella información que sea necesaria para la realización de las tareas según el rol que se posea en la empresa.
- Solo se debe generar los accesos a los recursos que sean necesarios para el tratamiento de la información según el cargo o rol que se desempeñe.
- Generar la documentación en la cual se pueda definir las responsabilidades que ayuden a gestionar e identificar a los custodios de la información.

- Concientizar al personal sobre la no divulgación de las credenciales otorgadas por parte de la empresa.
- Asegurar la confidencialidad de la información que se trasmite entre los usuarios de la red interna de la empresa.
- Gestionar los accesos solo al personal autorizado a la red interna que posee la empresa mediante los mecanismos de control que se posee.
- Genera un proceso para la gestión de los identificadores de los usuarios los cuales ayudan a identificar las responsabilidades de las acciones de los empleados.
- Eliminar de forma inmediata los identificadores de los usuarios que se hayan desvinculado de la institución.
- Se debe adaptar los derechos de accesos a los usuarios que han cambiado de rol o de tarea.
- Generar la documentación necesaria para poder mantener un registro de los derechos de acceso que poseen los usuarios a los sistemas y servicios que fueron concedidos a los usuarios.
- Se debería incluir clausulas en los contratos en los cuales se indique las sanciones en caso de que el personal o los contratistas intenten ingresar de forma no autorizada.
- Se debe revisar regularmente las competencias que tienen los usuarios que posee accesos privilegiados.
- Se debe crear un procedimiento el cual ayude a la verificación de la identidad de un usuario antes de proporcionarle la información que le ayude a la autentificación ya sea temporal o de sustitución.
- Cuando se trabaje con sistemas o software de terceros se debe cambiar de forma inmediata la información de autenticación que viene por defecto.
- Para el personal que posee accesos privilegiados se debe implementar un proceso de revisión frecuente.
- Se debe cambiar la información de autenticación cuando exista indicios de una posible fuga de información.
- Cuando se usen contraseñas secretas de autenticación se deben utilizar contraseñas de calidad, que posea una longitud mínima y además sean:
    - Fáciles de recordar
    - Que no incluya información personal
    - Que no está basada en objetos que se usa con frecuencia

○ Que los caracteres que conformen las contraseñas no sean consecutivos ○ Que las contraseñas que se emplee sean las mismas para lo laboral y lo personal • Se debe proporcionar los controles de acceso físico o lógico para aislar las aplicaciones, los datos de las aplicaciones y los sistemas.
RESPONSABILIDADES:
• Todos los gerentes deben asegurar que el personal que se encuentre bajo su cargo reciba los accesos y tengan conocimiento de las políticas y de cumplimiento a las mismas. • Cada persona que sea responsable de un equipo de computación debe dar cumplimiento a las políticas de seguridad. • El departamento de tecnología debe bridar las herramientas adecuadas para poder tener los accesos.

Fuente: [39]

Política para la gestión de los controles criptográficos

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE LOS CONTROLES CRIPTOGRÁFICOS		
OBJETIVO:	Garantizar el uso adecuado de los controles criptográficos para proteger de forma correcta la integridad, la confidencialidad y la autenticidad de la información.	
ALCANCE:	Esta política está diseñada para toda la información que requiera ser protegida de forma correcta para de esta manera mantener la integridad, autenticidad y confidencialidad de esta.	
REFERENCIA:	10.1. controles criptográficos. 10.1.1. política de uso de los controles criptográficos. 10.1.2. Gestión de claves.	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		
• Como primera instancia se debe identificar las circunstancias en las cuales sea necesario la implementación de los controles criptográficos y las personas encargadas para la administración y gestión de las claves.		

- Se debe generar una evaluación de los riesgos a los cuales está expuesto la empresa y con los resultados obtenidos generar el nivel de cifrado que se necesita.
- Se debe implementar algoritmos de cifrado que sean de un estándar internacional.
- Cuando las entidades externas necesiten usar los sistemas de información de la empresa se debe implementar técnicas criptográficas desde la autenticación del usuario.
- Para la trasmisión de información se debe utilizar canales de comunicación que sean seguros tales como SSL/TLS.
- Toda la información que sea trasladada a través de medios extraíbles debe poseer un código de protección el cual ayude a resguardar los registros que se trasladan en dichos medios.
- El encargado de la generación de las claves criptográficas será el único que se podrá encargar de la generación y distribución de los códigos de acceso a los archivos o equipos que se encuentran encriptados.
- Para la generación de la encriptación se deberá realizar una solicitud al encardado de la administración de las claves criptográficas ya que sin su autorización no se podrá realizar dicha acción.
- Todas las claves criptográficas deben estar protegidas en contra de la divulgación, modificación y destrucción. Ya que las acciones antes mencionadas solo pueden ser ejecutadas por el encargado de la generación de las claves.
- Se debe establecer un tiempo de vida útil que tendrán las claves criptográficas, este tiempo dependerá según el contexto en el que se emplee las claves.

RESPONSABILIDADES:

- Los responsables de la seguridad de la información deben ser los encargados de velar por el cumplimiento de esta política.
- El departamento de seguridad debe capacitar de forma periódica a el personal para que este comprenda la importancia de mantener un correcto uso de los controles criptográficos.
- Ultralink será el encargado de proporcionar todas las herramientas que sean necesarias para garantizar la protección de los equipos que se necesitan para la generación y almacenado de las claves.

Fuente: [39] [42]

Política para la gestión de la seguridad en las operaciones

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad

POLÍTICA DE SEGURIDAD EN LAS OPERACIONES	
OBJETIVO:	El objetivo de la presente política es asegurar que el funcionamiento de las instalaciones en las cuales se da tratamiento a la información sea seguro y permitan generar los registros de los eventos.
ALCANCE:	Esta política de seguridad es aplicable para el personal que se encarga de preparar y gestionar los cambios en la documentación de los procedimientos operacionales, también incluye al personal que se encarga de gestionar los registros de las actividades que se generan en el sistema.
REFERENCIA:	12.1. Responsabilidades y procedimientos de operación. 12.1.1. Documentación de procedimientos de operación. 12.1.2. Gestión de cambios. 12.4.1. Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema.

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Se debería documentar los procedimientos en los cuales estén asociados los recursos de tratamiento y comunicación de la información, entre esos procesos estarían la generación de copias de seguridad, el mantenimiento de los equipos, el encendido y apagado de los ordenadores, la gestión de los soportes, etc.
- Se debe documentar las instrucciones que se empelan para el manejo de los errores u alguna eventualidad que puedan generarse en la ejecución de los sistemas que posee la empresa.
- En los procedimientos operativos se debe documentar de forma clara los procedimientos de recuperación y reinicio del sistema ya que esto ayuda a generar una pronta recuperación ante las amenazas.
- Se debe poseer la documentación para el manejo correcto de los resultados y en caso de que existan fallas en la obtención de estos su correcta destrucción.

- Debe existir una lista detallada de los contactos de soporte tanto interno como externo a los cuales se pueda consultar en caso de que se susciten consecuencias inesperadas.
- Los procedimientos operacionales deben tratarse como documentos formales ya que los únicos que podrían autorizar su modificación son las autoridades de la dirección.
- Cuando se realicen cambios estos deben ser controlados y documentados mediante la utilización de las solicitudes necesarias para su ejecución.
- Al implementar los cambios se debe planificar y contar con todas las herramientas necesarias para de esta forma mantener operativo el sistema de información que posee la empresa.
- Se debe establecer los procedimientos formales para la generación de las actualizaciones, los parches de las aplicaciones o cualquier cambio que afecte en la funcionalidad de los sistemas.
- Se debe generar la documentación de un plan de roll-back en el cual se incluya las actividades a seguir cuando se quiera cancelar los cambios y de esta forma poder volver al estado anterior.
- Se debe elaborar y revisar periódicamente los registros de las actividades de los usuarios que tengas acceso a la infraestructura, los servidores, los sistemas y las bases de datos para de esta forma poder tener una respuesta oportuna ante cualquier eventualidad.
- Ya que los registros de actividades pueden poseer información sensible se debe tomar las medidas adecuadas para poder tener la privacidad necesaria.
- Se debe registrar las actividades del administrador y operador del sistema para poder garantizar la protección contra los cambios no autorizados.

RESPONSABILIDADES:

- El encargado del a seguridad de la información será el que se encargue de velar por el cumplimiento de esta disposición.
- El encargado del departamento de TI será el responsable de dar seguimiento a todas las implementaciones que sean necesarias para la ejecución de esta política.
- el encargado de la infraestructura tecnológica será responsable de mantener los procedimientos e instructivos actualizados.

Fuente: [39] [43]

Política de seguridad contra software maliciosos

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad

POLÍTICA DE SEGURIDAD CONTRA SOFTWARE MALICIOSOS	
OBJETIVO:	Está política tiene como objetivo asegurar que los sistemas de información se encuentren protegidos contra los softwares maliciosos.
ALCANCE:	Está diseñada para todos los sistemas informáticos que ayudan en el soporte de los procesos que posee Ultralink.
REFERENCIA:	12.2. Protección contra códigos maliciosos. 12.6.2. Restricción en la instalación de software. 14.2.2. Procedimientos de control de cambios en los sistemas.

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Instalar y actualizar software de detección de virus como un método de precaución.
- Se deben definir procedimientos y controles que permitan detectar el uso de software no autorizados.
- Cuando se obtenga ficheros o cualquier soporte externo se debe realizar la comprobación ante códigos maliciosos antes de su uso.
- Se debe brindar al personal la capacitación sobre el correcto uso de los antivirus o de cualquier otro mecanismo que se emplee para la detección de software malicioso.
- Se debe capacitar a los usuarios para que sepan identificar y actual cuando se reciba una alarma de detección de software malicioso.
- En los sitios web se deben implementar controles los cuales ayuden a controlar el acceso a sitios maliciosos.
- Se debe implementar un análisis periódico de los sistemas informáticos en búsqueda de software malicioso.
- Se debe definir procedimientos y responsabilidades los cuales ayuden a la recuperación ante los ataques de códigos maliciosos.
- Se puede implementar el uso de más de dos productos de protección contra códigos maliciosos para obtener una mejor protección ante este tipo de códigos.

• Ya que el uso de software que ayudan a la detección de código malicioso no es suficiente se podría acompañar de procedimientos operacionales los cuales también ayuden a la prevención de estos códigos malicioso. • En caso de la detección de algún código malicioso se deben establecer procedimientos de aislamiento y recuperación ante el ataque. • Cuando se emplee los escaneos de seguridad se debe incluir los archivos adjuntos que se obtiene en los correos electrónicos y de las páginas web.
RESPONSABILIDADES:
• El responsable de la seguridad de la información es el encargado de velar por el correcto cumplimiento de la presente política. • El personal y los proveedores deben cumplir con lo establecido en la presente política.

Fuente: [39] [44]

Política para la creación de copias de seguridad

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE SEGURIDAD PARA LA CREACIÓN DE COPIAS DE SEGURIDAD		
OBJETIVO:	Está política tiene como objetivo verificar que se realice copias de seguridad de la información y del software las cuales garanticen la continuidad del negocio.	
ALCANCE:	Para todo el personal que se encuentra involucrado en la creación y supervisión de los respaldos de la información de la empresa.	
REFERENCIA:	12.3.1 Copias de seguridad de la información.	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		
• Se debe proporcionar los recursos adecuados para las copias de respaldo para de esta forma asegurar que toda la información y software que son esenciales puedan recuperarse ante cualquier desastre o fallo de los sistemas. • Se deben producir registros precisos y completos de las copias de respaldo y de los procedimientos de recuperación. • Las copias deberían almacenarse en un lugar alejado para de esta forma proteger las copias de los desastres naturales. • Los soportes que se generan deben ser probados periódicamente para asegurarse de que estos puedan ayudar en un caso de emergencia.		

• Cuando las copias que se generen sean de carácter confidencial estas deben estar protegidas mediante un cifrado. • Una vez que ya no se pueda reutilizar los medios en los cuales se almacena los respaldos se debe definir un procedimiento de reemplazo de los medios en los cuales se almacena las copias y su posterior destrucción. • En los equipos en los cuales se ejecuten las copias de la información se deben implementar los niveles de protección que indica el fabricante para tener una mejor protección. • Antes de implementar cambios en los Sistemas Operativos se debe implementar de forma inmediata las copias de información.
RESPONSABILIDADES:
• El departamento de seguridad de la información será el responsable de asegurar que se generen los respaldos de la información de forma confidencial. • El departamento de tecnología de la información se encargará de brindar un resguardo seguro de las copias de seguridad y ofrecer todos los medios necesarios para poder generar un almacenamiento optimo.

Fuente: [45] [39]

Política de seguridad en las comunicaciones

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES		
OBJETIVO:	El objetivo de esta política es garantizar la protección de la información que se trasmite mediante las redes además de la infraestructura que se emplea para el soporte de este proceso.	
ALCANCE:	Esta política se aplica a todo el personal de Ultralink que está relacionado con la manipulación de las redes o la trasmisión de información mediante las mismas.	
REFERENCIA:	13.1. Gestión de la seguridad en las redes. 13.2. Intercambio de información con partes externas. 13.2.3. Mensajería electrónica. 13.2.4. Acuerdos de confidencialidad y secreto.	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		

- Se deben establecer las responsabilidades y los procedimientos para la gestión de los equipos de red.
- Se debe implementar un registro de eventos y monitorización de estos para poder detectar acciones que podrían afectar a la seguridad de la información.
- Se deben crear controles especiales para salvaguardar la integridad y confidencialidad de los datos que transitan a través de las redes.
- Las conexiones que se realizan en los sistemas de red deben ser registrados y autenticados.
- Las actividades que se emplean para la gestión y organización de los servicios de red deben ser coordinados para que los controles que se empleen sean aplicados de forma correcta y consistente.
- Se debe crear procedimientos para la gestión de los equipos remotos, el acceso mediante VPNs, el redireccionamiento de puertos y el área de los usuarios finales.
- Se debe poseer un esquema de la red que posee la organización, este debe contener los enlaces de las redes y subredes.
- Se debe incorporar tecnología que ayude a proteger los servicios de red, como la autenticación, controles de conexión de red.
- Los proveedores de los servicios deben garantizar la seguridad de los servicios que ellos prestan a la empresa para de este modo poder evitar fallos en la red.
- Se deben crear controles o procedimientos para proteger la información sensible que se trasmite en archivos adjuntos.
- Cuando se necesiten permisos especiales o adicionales para utilizar las redes o servicios de red se deben enviar las solicitudes al departamento de TICs el cual se encargará de aprobar o rechazar dicha petición.
- Los usuarios con computadores personales que deseen utilizar los servicios de red en la deben ajustarse a los requisitos de esta política y deben mantener la configuración hasta el retiro del equipo de las redes de la Institución.
- Sólo el personal interno que sea formalmente autorizado puede hacer uso del sistema de correo electrónico.
- Se debe incluir mayores niveles de autenticación para proteger los mensajes contra los accesos no autorizados.
- Revisar que la dirección y el trasporte que se emplea para los mensajes sean los correctos.
- Se puede utilizar una forma estándar y limitación de espacio de almacenamiento para cada usuario que utilice el servicio de correo. Si existe

alguna excepción esta debe ser autorizada por el encargado del departamento de TICs.

- Es responsabilidad de cada usuario de correo revisar y eliminar los mensajes que se han detectado como SPAM.
- En caso de que la comunicación lo amerite los correos que se envíen deben ser firmados de forma digital e incluir controles formales que ayuden a la trasferencia segura de la información.
- El correo electrónico no debe ser empleado para el envío de mensajes que no estén relacionados con las actividades que se ejecutan en la institución.
- Se debe hacer una limpieza periódica de la bandeja de recibidos para de esta forma limpiar el almacenamiento que posee el correo y también de esta forma se reduce los riesgos de que otra persona pueda acceder a la información que se trasmite.
- Cuando la información que se vaya a transferir por la red, se deben crear acuerdos de confidencialidad los cuales deben cumplir las partes interesadas.
- Al momento de generar los acuerdos de confidencialidad se debe controlar que estos sean firmados de forma manual o digital ya que al no existir la firma en estos documentos estos acuerdos no tendrán validez.
- El área de recursos humanos será la encargada de gestionar estos acuerdos sean estos físicos o digitales.

RESPONSABILIDADES:

- El encargado del departamento de TICs será el responsable de autorizar y controlar la implementación de esta política.
- El comité de seguridad de la información será el encargado de supervisar la correcta implementación de esta política.
- El encargado de la infraestructura de tecnología será el responsable de mantener actualizados los procedimientos que se generen al implementar esta política.
- El personal de la empresa Ultralink será el responsable de cumplir esta política.

Fuente: [46] [39]

Política de seguridad para escritorios y pantallas limpias

		Departamento de seguridad
POLÍTICA DE SEGURIDAD PARA ESCRITORIOS Y PANTALLAS LIMPIAS		
OBJETIVO:	Es generar una política para prevenir el acceso no autorizado a los equipos o el daño de la información que se encuentre en los mismos durante y fuera del horario de trabajo	
ALCANCE:	Aplica para todos los empleados de la institución que tengan acceso a un computador.	
REFERENCIA:	11.2.8. Equipos informáticos desatendidos. 11.2.9. política de puesto de trabajo despejado y bloqueo de pantalla	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		

- Al abandonar el puesto de trabajo y al finalizar la jornada laboral se debe despejar todos los documentos físicos o medios extraíbles que contengan información, estos deben ser guardados en un lugar seguro y bajo llave.
- Durante las horas de trabajo los puestos de labores deben permanecer limpios y ordenados.
- Los dispositivos que se empleen para la impresión o digitalización de documentos deben permanecer sin documentos.
- Los cajones o archivadores que contengan documentos con información deben permanecer cerrados durante la hora de almuerzo y al finalizar la jornada.
- Al levantarse del lugar de trabajo se debe bloquear la sesión de los equipos para de esta forma proteger el acceso no autorizado a los aplicativos o servicios que posee la institución.
- El departamento de TICs debe implementar el bloqueo automático de la sesión de usuarios luego de trascurrir los 5 minutos de inactividad en el equipo de cómputo.
- Cuando los equipos de cómputo, impresión y digitalización no se los estén utilizando estos deben ser apagados.
- El personal debe velar que los equipos de cómputo no estén expuestos a alimentos, bebidas, velas, el consumo de cigarrillo, etc.
- No se debe escribir las contraseñas ni otro dato importante en papeles o documentos que se encuentren a la vista.
- El personal no tiene el permiso de manipular las estaciones de trabajo o los computadores portátiles que no estén a su responsabilidad.

• Si el empleado está ubicado cerca de una zona a la cual tiene acceso los clientes, al ausentarse este debe guardar toda la documentación y medios físicos que posean información de uso interno. • El empleado no debe guardar documentos o información importante en la pantalla de inicio. • Para desactivar el protector de pantalla se debe ingresar la contraseña que se le generó al ser entregado el equipo. • Una vez se haya finalizado la jornada de trabajo el empleado deberá apagar la estación de trabajo. • No se deben colocar autoadhesivos ni ninguna figura en la pantalla del equipo de cómputo. • Se debe realizar el proceso de autenticación cuando el equipo de trabajo se lo encienda, reinicie o se lo bloquee.
RESPONSABILIDADES:
• El departamento de TICs debe encargarse de implementar las herramientas necesarias para bloquear los escritorios de los equipos de cómputo. • El departamento de seguridad de la información debe velar por el cumplimiento de la política. • Todos los empleados que tengan en su posición un equipo de cómputo o utilicen un dispositivo de impresión o digitalización deben cumplir con esta política.

Fuente: [47] [48] [39]

Política para el uso de internet, dispositivos móviles y redes sociales

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE SEGURIDAD PARA EL USO DE INTERNET, DISPOSITIVOS MÓVILES Y REDES SOCIALES		
OBJETIVO:	El objetivo de esta política es asegurar el uso del internet, los dispositivos móviles y las redes sociales para los propósitos relacionados con la empresa tomando en cuenta las medidas de seguridad para la protección de la información.	

ALCANCE:	Esta política va dirigida para todo el personal de la empresa los cuales deben cumplir esta política para hacer uso del internet, los dispositivos móviles y las redes sociales dentro de la empresa.
REFERENCIA:	9.1.1. Políticas de control de acceso. 9.1.2. Control de acceso a las redes y servicios asociados. 8.1.3. Uso aceptable de los activos.

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Se debe utilizar el internet exclusivamente para actividades que ayuden a desarrollar las labores de la empresa.
- El empleado que requiera el uso del internet deberá enviar una solicitud al departamento de seguridad el cual será el encargado de autorizar o negar esta solicitud dependiendo de la tarea a realizar.
- La empresa Ultralink se reserva el derecho a restringir el acceso total o parcial a sitios web.
- Toda información que se trasmita por el internet puede ser monitoreada para su posterior revisión.
- Está prohibido visitar sitios de entretenimiento o de divulgación de información.
- Todos los archivos que sean obtenidos del internet antes de su ejecución deben ser examinados por un antivirus.
- Las actualizaciones de software solo deben ser realizadas por el departamento de tecnología de la información.
- No se permite la descarga o instalación de juegos, películas, videos, software de libre distribución o algún producto que pueda atentar contra la seguridad de la información.
- Se debe llevar un registro en el cual se especifique el estado de todos los dispositivos móviles que posee la entidad.
- Cuando al empleado se le asigna un dispositivo móvil para el desarrollo de las tareas se debe hacer buen uso de estos.
- Los dispositivos móviles que salgan de la institución deben tener implementados controles de seguridad los cuales ayuden a proteger la información y la ejecución de aplicaciones que puedan atentar contra la seguridad de los dispositivos.
- Todos los dispositivos móviles deben poseer un sistema de autenticación el cual ayude a proteger el almacenamiento de la información en estos dispositivos.

• Todos los dispositivos que pertenezcan a la empresa podrán ser monitoreados y sometidos a los controles de seguridad para proteger esos dispositivos ante algún ataque malicioso. • Las contraseñas que se empleen para el ingreso a las redes sociales deben ser robustas lo cual ayude a la protección de la información que se trasmita mediante esta red. • La empresa será la encargada de definir que se puede publicar o no en sus redes sociales ya que la imagen que se refleja es la imagen de la empresa. • Todos los usuarios que tengan permiso de utilizar las redes sociales deben ser responsables de las practicas que ejecuten y que puedan comprometer la seguridad de la entidad. • Es permitido la utilización de las redes sociales para realizar video conferencias o streaming siempre y cuando estas actividades no interfieran con las operaciones normales de la empresa. • Cuando se esté utilizando las redes sociales no se debe descargar ningún archivo o ejecutable ya que estos pueden contener algún código malicioso.
RESPONSABILIDADES:
• Todo empleado que tenga asignado un equipo de cómputo o un dispositivo móvil tiene la responsabilidad de cumplir esta política de seguridad. • Todos los gerentes deben asegurar que el personal que se encuentre bajo su cargo conozca esta política y le den cumplimiento. • El departamento de tecnología de la información debe brindar las herramientas necesarias para dar protección y accesos a internet y las redes sociales.

Fuente: [47] [39] [49]

Política de seguridad en relación con los proveedores

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE SEGURIDAD EN RELACIÓN CON LOS PROVEEDORES		
OBJETIVO:	El objetivo de esta política es asegurar la protección de los activos que posee la organización cuando estos sean accesibles a los proveedores	
ALCANCE:	Esta política aplica para todos los proveedores que pueden acceder a los activos que posee la empresa	

REFERENCIA:	15.1. 1.Política de seguridad de la información para suministradores. 15.1.2. Tratamiento del riesgo dentro de acuerdos de suministradores. 15.2.1. Supervisión y revisión de los servicios prestados por terceros. 15.2.2. Gestión de cambios en los servicios prestados por terceros.

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Se debe documentar todos los acuerdos que se generen con los proveedores para asegurar que no haya malentendidos entre las partes interesadas.
- Una vez que el acuerdo haya finalizado debemos asegurarnos de que este ya no pueda ingresar a la información de la empresa.
- En los acuerdos que se generan entre la empresa y los proveedores se debe especificar la penalización en caso de incumplimiento o las garantías que tendrán cada una de las partes interesadas.
- Se debe listar el personal de los proveedores el cual puede acceder a la información que posee la empresa, cuáles son las condiciones para que ellos puedan obtener la información.
- En el caso de subcontratación se debe incluir los controles necesarios y pertinentes para que no exista una mala utilización de la información que posee la empresa.
- En la documentación que se genera para los acuerdos debe constar las obligaciones que deben cumplir los proveedores con respecto a la seguridad de la empresa.
- La empresa debe controlar y revisar de forma periódica los servicios que son suministrados por el proveedor y de esta forma verificar el cumplimiento de los acuerdos.
- Se debe tener en consideración los cambios que se generen en los acuerdos con los proveedores.
- Se debe documentar las actualizaciones o modificaciones a las políticas o procedimientos que estén relacionados con los proveedores.
- Cuando existan cambios tecnológicos por parte de los proveedores y afecten a la empresa esta debe ser informada.
- Cuando se genere un inconveniente por parte del proveedor se debe exigir un informe sobre la eficacia del servicio y de los controles implementados para corregir el error.

RESPONSABILIDADES:
• Esta política debe ser cumplida por todos los proveedores que tengan alguna relación con la empresa Ultralink. • El departamento de seguridad de la información debe dar seguimiento y control al cumplimiento de esta política.

Fuente: [39] [50]

Política para la gestión de incidentes de seguridad de la información

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad
POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
OBJETIVO:	El objetivo de esta política es gestionar y solucionar de forma adecuada todos los incidentes de seguridad que se reporten en Ultralink.	
ALCANCE:	Se aplica para todos los empleados y proveedores de Ultralink que detecten un incidente de seguridad el cual deben reportar	
REFERENCIA:	16.1.1. Responsabilidades y procedimientos. 16.1.3. Notificación de puntos débiles de la seguridad. 16.1.5. Respuesta a los incidentes de seguridad. 16.1.6. Aprendizaje de los incidentes de seguridad de la información.	
CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:		
• Se debe establecer responsabilidades para garantizar la gestión de los procedimientos de preparación y planificación de las respuestas ante algún incidente. • Se debe establecer procedimientos de monitorización, detección, análisis y comunicación de los incidentes de seguridad que puedan afectar a la empresa. • Desarrollar procedimientos para la evaluación de los puntos débiles de seguridad y su posterior procedimiento de solución. • Se debe contar con personal competente el cual pueda manejar de forma eficiente los incidentes de seguridad. • Los empleados o personal externo deberían ser obligado a notificar cualquier punto débil que se observe en los sistemas o servicios que posee la empresa.		

• Los mecanismos de comunicación que se empleen para notificar sobre las debilidades deben ser de fácil acceso y de gran disponibilidad. • Todos los empleados que sospechen de algún incidente no deben solucionarlo ellos mismo sino deben informar al personal calificado al cual se le ha asignado dicha responsabilidad. • El personal que este encargado de la solución de los incidentes debe capacitarse constantemente ya que las amenazas están en constante evolución. • Ante algún incidente se debe recoger la evidencia lo más pronto posible para de esta forma tener una respuesta inmediata. • Hay que evaluar si la empresa posee la capacidad para resolver los incidentes o necesita ayuda de terceros. • Cuando se ejecute alguna acción para solucionar un incidente esta debe ser documentada para de esta forma saber cuáles son los resultados obtenidos. • Se debe documentar el incidente desde la detección, su tratamiento y si ha sido satisfactoriamente cerrado. • Se debe realizar entrenamientos de seguridad los cuales ayuden a evitar los incidentes y su correcta gestión. • El conocimiento que se obtiene de incidentes anteriores debe ser empelado para reducir la probabilidad de incidentes en el futuro. • Se debe generar una bitácora en la cual se reporten los incidentes atendidos por la entidad.
RESPONSABILIDADES:
• El departamento de seguridad de la información debe velar por el cumplimiento de esta política. • Todos los empleados y proveedores deben cumplir con los procedimientos e instructivos que se menciona en esta política.

Fuente: [39] [51]

Política de seguridad de cumplimiento

ULTRALINK Más internet, más velocidad	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN:** 1.0
		RESPONSABLE: Departamento de seguridad y Talento Humano
POLÍTICA DE SEGURIDAD DE CUMPLIMIENTO		

OBJETIVO:	Esta política está diseñada para evitar el incumplimiento de las disposiciones legales y los reglamentos relacionados a la seguridad de la información.
ALCANCE:	Se aplica para todos los empleados de la empresa y proveedores que tengan relación directa con Ultralink.
REFERENCIA:	18.1.3. Protección de los registros de la organización. 18.1.4. Protección de datos y privacidad de la información personal. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.

CRITERIOS PARA LA IMPLEMENTACION DE LA POLÍTICA:

- Los registros deben estar protegidos ante pérdidas, falsificación, destrucción o acceso no autorizado.
- Si se escoge como almacenamiento los soportes electrónicos se debe establecer procedimientos los cuales aseguren el acceso a los datos ante las pérdidas que se pueden generar por cambios de la tecnología.
- Los sistemas que se empleen para el almacenamiento de los registros deben garantizar su identificación y retención además de permitir la destrucción adecuada de los registros cuando estos ya no sean necesarios.
- Se debe mantener un inventario sobre las fuentes de información clave y se debe determinar en este inventario el tiempo de utilidad de estas fuentes.
- Se debe implementar un control el cual garantice la protección y privacidad de los datos personales suministrados a la empresa.
- Los gerentes de cada departamento deben ser os responsables de dar cumplimiento a todos los procedimientos de seguridad que sean aplicables en su área de trabajo.
- Cuando se identifiquen incumplimientos se debe identificar las causas de este evento, posterior a eso se debe evaluar la necesidad de tomar acciones correctivas.
- Cuando se generen actualizaciones de los sistemas se debe identificar los fallos y documentarlos.
- Se debe establecer medidas correctivas antes de que los fallos puedan terminar en una amenaza real para los sistemas que posee la empresa.
- Para las revisiones técnicas se debe tener en cuenta la utilización de sistemas los cuales estén constituidos por herramientas que generen informes y

mediciones automáticas que ayuden a solucionar los requerimientos de la empresa. • Toda revisión de carácter técnica solo debe ser implementada por personal calificado y autorizado en el caso de que el personal este ocupado este debe supervisar a la persona que haya delegado para dicha acción. • Cuando se realicen pruebas de seguridad a los sistemas se debe tener cuidado en comprometer la seguridad del sistema, además estas deben ser planificadas y documentadas. • Se debe analizar los sistemas operativos para garantizar que los controles implementados se estén ejecutando de forma correcta, para la realización de esta verificación se necesita de personal calificado.
RESPONSABILIDADES:
• El personal y los proveedores deben cumplir con todos los lineamientos mencionados dentro de esta política. • El departamento de seguridad de la información debe velar por el cumplimiento de esta política. • Cada gerente debe encargarse de que cada persona bajo su control cumpla con los lineamientos expuestos en la política.

Fuente: [39]

Anexo 19. Certificados de aprobación por parte de Ultralink

ULTRALINK
Mas Internet, mas velocidad

Quito, 01 de abril de 2021

CERTIFICACIÓN

Yo Santiago Llumiquinga certifico haber leído y aprobado el primer entregable, estando de acuerdo en el CONTENIDO y FORMATO del trabajo de titulación de: PROPUESTA DE DISEÑO DE UN SGSI BASADO EN LA NORMA ISO/IEC 27001. CASO DE ESTUDIO LA EMPRESA ULTRALINK por los señores Marco Vinicio Guacanés Castro y Jonathan Alexander Vilatuña Morales.

Atentamente,

Ing. Santiago Llumiquinga
Jefe de departamento técnico

TELECOMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN
SIGNAL TELECOM